Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik

Schulze, Matthias

Veröffentlichungsversion / Published Version
Forschungsbericht / research report

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

Empfohlene Zitierung / Suggested Citation:
Schulze, M. (2019). *Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik.* (SWP-Studie, 10/2019). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://doi.org/10.18449/2019S10

SWP-Studie

Matthias Schulze

Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik

Stiftung Wissenschaft und Politik
Deutsches Institut für
Internationale Politik und Sicherheit

SWP-Studie 10
Mai 2019, Berlin

Sicherheitslücken in Hard- und Software sind ein globales, kollektives Problem der Cyber-Sicherheit. Durch die fortschreitende Digitalisierung der Lebenswelt und digitale Rüstungswettläufe steigt die Verwundbarkeit, vor allem der Industriestaaten. Gleichzeitig beharren offensive Cyber-Akteure darauf, dass die Ausnutzung unbekannter sogenannter 0-Day-Sicherheitslücken für militärische Cyber-Operationen, aber auch zum Zweck der Spionage und der Strafverfolgung essentiell sei.

Ein konstruktiver Umgang mit diesem Offensiv-defensiv-Dilemma, das sich für die Staaten beim Handling von 0-Day-Sicherheitslücken auftut, findet bisher in der deutschen Cyber-Sicherheitspolitik nicht statt. Die Bundesregierung sollte eine proaktivere Schwachstellen-Governance entwickeln. Sie sollte die Praxis der staatlichen Akquise und Verwendung von Sicherheitslücken überdenken, auf die Verkürzung der Lebenszeit von Schwachstellen hinarbeiten und die negativen Externalitäten einer offensiven Cyber-Sicherheitspolitik reflektieren. Deutschland und die EU sollten statt Geheimhaltung einen offeneren Umgang mit Schwachstellen kultivieren. Dazu gehört die Einführung verpflichtender Meldeprogramme für private und öffentliche Organisationen, die Bereitstellung von Bug-Bounty-Plattformen und die Regulierung schwarzer Schwachstellenmärkte.

SWP-Studie

Matthias Schulze

Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik

Stiftung Wissenschaft und Politik
Deutsches Institut für
Internationale Politik und Sicherheit

SWP-Studie 10
Mai 2019, Berlin

SWP-Studien unterliegen einem Verfahren der Begutachtung durch Fachkolleginnen und -kollegen und durch die Institutsleitung *(peer review)*, sie werden zudem einem Lektorat unterzogen. Weitere Informationen zur Qualitätssicherung der SWP finden Sie auf der SWP-Website unter https://www.swp-berlin.org/ueber-uns/qualitaetssicherung/. SWP-Studien geben die Auffassung der Autoren und Autorinnen wieder.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-200
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6372
doi: 10.18449/2019S10

Inhalt

Dr. Matthias Schulze ist Wissenschaftler in der Forschungsgruppe Sicherheitspolitik

Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik

Zahlreiche staatliche und nicht-staatliche Akteure entwickeln gegenwärtig Fähigkeiten für offensive Cyber-Operationen, Spionage und Internetkriminalität. Komplexe, gezielte Cyber-Angriffe basieren in der Regel auf dem Ausnutzen unbekannter sogenannter 0-Day-Schwachstellen in der Hardware und im Softwarecode von Zielsystemen. Weil es gegen 0-Day-Cyber-Angriffe keine Abwehrmöglichkeit in Form eines Sicherheitspatches gibt, haben diese Attacken ein geringes Entdeckungsrisiko bei hoher Wirksamkeit. Aus diesem Grund halten Akteure, die Sicherheitslücken offensiv verwerten wollen, ihr Wissen darüber geheim (»stockpiling«) und entwickeln daraus 0-Day-Angriffstools (»0-Day exploits«). Die Konsequenz davon ist, dass solche Lücken nicht dem Hersteller gemeldet und folglich nicht behoben werden.

Sicherheitslücken können von jedem ausgenutzt werden, der sie kennt, was sie sowohl für Staaten als auch für die organisierte Kriminalität und böswillige Hacker interessant macht. Informationen über Sicherheitslücken und Exploits werden daher zu hohen Preisen auf Schwarzmärkten verkauft. Auf diese Weise wird die Proliferation von Cyber-Angriffstools vorangetrieben. Akteure mit eigentlich geringen Cyber-Fähigkeiten können dadurch zu formidablen Cyber-Angreifern werden. Durch staatliche Cyber-Angriffe und Cyber-Kriminalität entsteht jedes Jahr, je nach Schätzung, weltweit ein wirtschaftlicher Schaden in Höhe von 600 Milliarden US-Dollar. Durch das massenhafte Zurückhalten von Sicherheitslücken und die fortschreitende Digitalisierung der Lebenswelt steigt die digitale Verwundbarkeit der Industriestaaten, da Software immer mehr Aspekte des Alltags steuert.

Umgekehrt gilt, dass die Sicherheit größer wird, je mehr Sicherheitslücken gefunden und von den Herstellern geschlossen werden. In einer globalisierten Welt verwenden staatliche Behörden (Parlamente, Militärs und Nachrichtendienste) und Bürger die gleiche serienmäßig vertriebene (»off the shelf«-) Hard- und Software, etwa Microsoft Windows. Daher ist unsichere Software voller Sicherheitslücken ein weltweites strukturelles Problem der Digitalisierung.

Wenn Staaten ein Interesse an mehr Cyber-Sicherheit haben, müssen sie folglich ihren eigenen Umgang

mit dem Problem der Sicherheitslücken überdenken. Dies gilt erstens für die Akquise von Exploits. Zweitens müssen sie sich mit der Frage auseinandersetzen, ob sie selbst gefundene oder eingekaufte Lücken an Hersteller melden oder nicht. Und drittens sollten die Staaten ihre Haltung zum Bereich der »exploitation« definieren, also zu der Frage, ob und in welcher Form sie Schwachstellen für eigene Cyber-Operationen bzw. staatliches Hacking verwenden wollen und welche negativen Effekte damit verbunden sein könnten.

Staaten haben ein breites Spektrum an Handlungsoptionen. Die defensivste Variante wäre, das Wissen über eine Schwachstelle vollständig zu veröffentlichen (»responsible disclosure«), damit der Hersteller diese beheben kann. Die offensivste Option besteht in der Geheimhaltung und Verwendung von 0-Day-Sicherheitslücken für eigene Cyber-Angriffe. Dass aus der offensiven Ausnutzung von Schwachstellen grundsätzliche Probleme erwachsen, erkennen mittlerweile immer mehr Staaten an. In den USA haben die wichtigsten Institutionen des Sicherheitssektors daher seit 2008 unter dem Namen »Vulnerabilities Equities Process« (VEP) ein Verfahren zum Umgang mit Sicherheitslücken entwickelt: Dabei werden die entdeckten 0-Day-Schwachstellen einem Review unterzogen, bei dem offensive und defensive Akteure gemeinsam darüber beraten, ob die Lücke an den Hersteller gemeldet wird oder für eigene Cyber-Operationen verwendet werden darf. Auch in Deutschland haben im Herbst 2018 unter der Schirmherrschaft des Bundesministeriums des Innern Planungen begonnen, einen deutschen VEP-Prozess zu initiieren.

Obwohl die Etablierung eines solchen behördlichen Schwachstellenmanagementprozesses zu begrüßen ist, löst man damit nur einen kleinen Teil des strukturellen Problems der Sicherheitslücken. Die deutsche Cyber-Sicherheitspolitik sollte weiter denken. Dazu gehört, zu erkennen, dass das Schwachstellenproblem nicht nur ein technisches und innenpolitisches Problem der Exekutive ist, sondern dass es eine soziale, ökonomische und geopolitische Komponente hat und als Herausforderung nur global gelöst werden kann. Deutschland sollte eine proaktive Politik der *Schwachstellen-Governance* verfolgen. Das bedeutet, dass die Bundesregierung sich zu einer politischen Steuerung des strukturellen Schwachstellenproblems in den folgenden Bereichen entschließen sollte:

- Erstens wäre die Kontrolle und Transparenz der *staatlichen Akquise* (Entdeckung oder Einkauf, Ausnutzung und Lagerung) von 0-Day-Sicherheitslücken und von Exploits zu erhöhen, die militärischen Cyber-Operationen, der Strafverfolgung oder der Auslandsspionage dienen.
- Zweitens müsste sich die Bundesregierung die *Minimierung der Existenz und der Lebenszeit aller Schwachstellen* in IT-Systemen zum Ziel setzen, die die eigene Bevölkerung betreffen.
- Drittens bedarf es einer *politischen Steuerung bzw. Minimierung der negativen externen Effekte des Schwachstellenökosystems*. Das gilt vor allem für die Dynamik auf den weißen und schwarzen Märkten für Schadsoftware und Schwachstellen und für die Auswirkungen auf die internationalen Beziehungen.

Die vorliegende Studie liefert Vorschläge, wie eine solche Schwachstellen-Governance aussehen könnte:

- Erstens sollten Maßnahmen ergriffen werden, um schneller mehr Schwachstellen zu entdecken und zu schließen. Dazu sollten öffentliche und private Organisationen »Coordinated Vulnerability Disclosure«-Programme einführen, die es ethischen Hackern ermöglichen, in öffentlichen Systemen gefundene Sicherheitslücken an die betroffenen Organisationen zu melden. Diese Organisationen verpflichten sich, die gemeldeten Lücken schnellstmöglich zu schließen.
- Sodann sollte dafür gesorgt werden, dass weniger Lücken auf grauen und schwarzen Märkten illegal gehandelt werden. Ein erster Schritt wäre hier, ein Gegengewicht zu den Schwarzmärkten zu schaffen. Europa sollte Schwachstellenforscher nicht kriminalisieren und den Aufbau europäischer Plattformen für die Meldung von Schwachstellen (Bug Bounty Platforms) und Hackerwettbewerbe unterstützen, auf denen ethische Hacker Lücken für eine Belohnung melden können (sogenannte weiße Märkte). Ferner sollten Mittel bereitgestellt werden, um die Prämien zu erhöhen, die auf solchen weißen Märkten ausgezahlt werden.
- Die EU und ihre Mitgliedstaaten könnten Unternehmen verpflichten, die Informationen über Sicherheitslücken, die sie betreffen, auf Schwarzmärkten einzukaufen und die Fehler zu beheben. Es sollte geprüft werden, inwiefern es sinnvoll ist, dass ökonomisch starke Staaten das 0-Day-Schwachstellenangebot auf Schwarzmärkten leerkaufen.

Letztlich ist ein Paradigmenwechsel erforderlich hin zu einem proaktiveren Umgang mit Schwachstellen. Organisationen sollten in ihren Systemen entdeckte Schwachstellen nicht als ein Imageproblem betrachten, das es zu verheimlichen gilt, sondern als neue Normalität anerkennen.

Das Sicherheitslückendilemma

Moderne Hard- und Software ist aufgrund ihrer Komplexität fehleranfällig. Betriebssysteme wie Windows 7 enthalten circa 40 Millionen und Googles Internetdienste rund 2 Milliarden Zeilen Code.[1] Es wird geschätzt, dass in rund 1000 Zeilen Programmcode zwischen 10 und 20 Fehlern zu finden sind.[2] Solche Bugs sind dann eine Sicherheitslücke, wenn sie für schädliche Zwecke missbraucht werden können. Sicherheitslücken sind ein nahezu unvermeidbares Nebenprodukt, das bei der Softwareherstellung entsteht.

Die Komplexität und die Reichweite einer Sicherheitslücke bestimmen den Schweregrad und damit die Gefahr, die von einem sogenannten Exploit ausgeht, einem Tool, mit dem die Schwachstelle ausgenutzt werden kann.[3] Der Schweregrad des mit der Schwachstelle verknüpften Risikos kann nach gängigen Typologien von gering, mäßig, hoch bis hin zu kritisch reichen.[4] Kritische Sicherheitslücken erlauben das Ausführen von Schadcode ohne vorherige Nutzerinteraktion, zum Beispiel in Form eines Mausclicks.

Definition »Sicherheitslücke«

Unter einer IT-Schwachstelle bzw. *Sicherheitslücke* versteht man gemeinhin einen Fehler (»bug«) im Programmcode eines informationstechnischen Systems, der von Angreifern ausgenutzt werden kann, um in einem System nichtintendierte Effekte zu produzieren (wie etwa schädlichen Code auszuführen). Als »*0-Day-Schwachstelle*« bezeichnet man einen Fehler in einem IT-System, für den noch kein Software-Update bzw. kein Patch (engl. to patch = flicken) bereitgestellt wurde, der die Schwachstelle behebt. Der Hersteller hat sinnbildlich genau 0 Tage Zeit, die Lücke mit einem Patch zu schließen, bevor sie ausgenutzt werden kann. Sobald der Softwarehersteller Kenntnis von der Lücke erhält, sei es durch eigene Qualitätssicherungsprozesse oder durch die Meldung von Seiten Dritter wie zum Beispiel IT-Security-Forschern, spricht man von »*N-Day*«-Schwachstellen. Erst wenn eine Schwachstelle dem Hersteller bekannt ist, kann sie beseitigt werden. Eine vom Hersteller bewusst platzierte Lücke nennt man Hintertür. Aufbauend auf der Kenntnis einer 0-Day-Lücke kann ein »*0-Day-Exploit*« entwickelt werden, also ein Code, der die entdeckte Schwachstelle ausnutzt. Exploits sind »weaponized vulnerabilities« (Schwachstellen, die wie eine Waffe genutzt werden), also Werkzeuge für Cyber-Operationen. Schwachstellen sind zudem eine leicht verbreitbare Wissensressource.

Besonders kritisch sind Lücken in Übertragungsprotokollen, die eine automatische Verbreitung von Schadsoftware ermöglichen (»wormable«). Komplexe Sicherheitslücken sind schwierig zu finden, während einfache Lücken auch mit automatischen Verfahren entdeckt werden können und daher weniger wertvoll sind. Je mehr verschiedene Systeme oder Softwareversionen von einer Lücke betroffen sind, desto schwerwiegender ist sie. Zu den historisch größten Schwachstellen gehörte zweifellos der Heartbleed Bug in einer kryptografischen Bibliothek des SSL-Verschlüsselungsverfahrens, der im Jahr 2014 rund ein Drittel

1 Aditya Tiwari, »How Many Lines of Code Are there in Google, Facebook, and Windows OS«, *Fossbytes*, 16.9.2016, <https://fossbytes.com/how-many-lines-of-code-are-there-in-google-first-space-shuttle-facebook/> (Zugriff am 5.2.2019).

2 Lillian Ablon/Andy Bogart, *Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, Santa Monica: Rand Corporation, 2017, S. 1, <https://www.rand.org/pubs/research_reports/RR1751.html> (Zugriff am 5.2.2019).

3 Technisch betrachtet kann auch eine vom Hersteller platzierte Hintertür oder ein Hauptpasswort eine 0-Day Schwachstelle sein, vgl. Dave Aitel, »Why NSA Critics Are Wrong about Internet Vulnerabilities Like ›Heartbleed‹«, *Business Insider*, 29.5.2014, <www.businessinsider.com/here-is-why-nsa-critics-are-wrong-2014-5> (Zugriff am 5.2.2019).

4 Siehe zum Beispiel das »Common Vulnerability Scoring«-System, das eine zehnstufige Schweregradskala zur Klassifizierung verschiedener Sicherheitslücken bietet, die sich in der Industrie durchgesetzt hat, siehe Peter Mell/Karen Scarfone/Sasha Romanosky, *A Complete Guide to the Common Vulnerability Scoring System, Version 2.0*, <https://www.first.org/cvss/cvss-v2-guide.pdf> (Zugriff am 5.2.2019).

aller Websites betraf.[5] Der Bug erlaubte das Auslesen von verschlüsselter Website-Kommunikation und war daher so etwas wie der Generalschlüssel zum World Wide Web.

Aufgrund dieses Schädigungspotentials interessieren sich militärische Cyber-Kommandos, Geheimdienste und Strafverfolgungsbehörden zunehmend für Sicherheitslücken. Schwachstellen ermöglichen es Cyber-Angreifern aus der Ferne, unbemerkt auf computerisierte Systeme zuzugreifen. Der Stuxnet-Wurm, der iranische Atomzentrifugen sabotierte, basierte auf vier unbekannten Sicherheitslücken in Windows-Systemen und in industriellen Steuerungsanlagen.[6] Sicherheitslücken erlauben es, Schutzmechanismen auf Zielsystemen, wie etwa die Datenverschlüsselung, zu durchbrechen, und sind somit auch für die Spionage relevant. Die sogenannte »Quellentelekommunikationsüberwachung« von Smartphones oder PCs durch Strafverfolgungsbehörden mittels Schadsoftware beruht ebenso auf der Ausnutzung von Sicherheitslücken. Das Aufspielen von Schadsoftware aus der Ferne gleicht technisch dem Prozedere bei einem Cyber-Angriff, wird aber zur Differenzierung gemeinhin »staatliches Hacking« genannt.[7] Staaten, die im Cyber-Space operieren, replizieren also das Vorgehen von Hackern und verwenden deren Werkzeuge. Komplexe, gezielte Cyber-Angriffe (»Advanced Persistent Threats«, APT) wie Spionageoperationen oder Attacken mit physischer Schadenswirkung basieren oft auf der Ausnutzung von 0-Day-Schwachstellen, eben weil es in diesen Fällen keine Abwehrmöglichkeit gibt. Erst mit der Bereitstellung eines Patches verliert eine 0-Day-Sicherheitslücke ihre Wirksamkeit für Cyber-Angriffe.[8]

Aus dieser Offensiv-defensiv-Dynamik, die den Cyber-Space prägt, erwachsen zwei Interessengegensätze, die Gegenstand dieser Studie sind: Cyber-Verteidiger haben ein Interesse daran, alle Lücken in ihren Systemen zu schließen und 0-Days an den Hersteller zu melden (Option »*disclosure*«, Meldung & Offenlegung). Stellt der Hersteller einen Patch bereit, werden alle aktualisierten Systeme gegen den Exploit immunisiert. Das Melden von Sicherheitslücken an den Hersteller dient somit der kollektiven Cyber-Sicherheit.

»Da jeder die gleiche Software benutzt, bedeutet uns zu schützen, jeden zu schützen. Den Gegner verwundbar zu halten, bedeutet, dass wir verwundbar bleiben.«

Cyber-offensive Akteure wie Nachrichtendienste, Militär und Strafverfolgungsbehörden haben aufgrund ihres Aufgabenprofils ein entgegengesetztes Interesse: Für sie ist es von Vorteil, wenn Lücken offen bleiben, damit Spionage, digitale Überwachung, offensive Cyber-Operationen weiter stattfinden können, ohne entdeckt zu werden.[9] Diese Akteure wollen Lücken nicht an den Hersteller melden, sondern das Wissen darum für einen zukünftigen Cyber-Angriff zurückhalten (Option »*stockpiling*«, Zurückhalten & Lagerung). Kriminelle und ausländische staatsnahe Hacker teilen dieses Interesse. Aus diesem Interessengegensatz erwächst das Offensiv-defensiv-Dilemma: Jede 0-Day-Lücke, die aus Gründen einer möglichen offensiven Ausnutzung nicht behoben wird, schwächt die eigene Cyber-Verteidigung, wenn die gleichen betroffenen Systeme verwendet werden.[10] Der IT-Sicherheitsexperte Bruce Schneier hat das Dilemma in treffender Weise auf den Punkt gebracht: »Es gibt keine Möglichkeit, gleichzeitig US-Netzwerke zu schützen und ausländische Netzwerke offen für Angriffe zu halten. Da jeder die gleiche Software benutzt, bedeutet uns zu schützen, jeden zu schützen. Den Gegner

5 Jai Vijayan, »The 10 Worst Vulnerabilities of the Last 10 Years«, *Dark Reading*, 5.6.2016, <www.darkreading.com/vulnerabilities---threats/the-10-worst-vulnerabilities-of-the-last-10-years/d/d-id/1325425> (Zugriff am 5.2.2019).

6 Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, New York 2014, S. 99.

7 Sven Herpig, *Government Hacking. Global Challenges*, Berlin: Stiftung Neue Verantwortung, Januar 2018, <https://www.stiftung-nv.de/sites/default/files/government_hacking_akt.feb_.pdf> (Zugriff am 5.2.2019).

8 Tara Seals, »Companies Take an Average of 100 – 120 Days to Patch Vulnerabilities«, *Infosecurity Magazine*, 1.10.2015, <https://www.infosecurity-magazine.com/news/companies-average-120-days-patch/> (Zugriff am 5.2.2019).

9 Rick Ledgett, »No, the U.S. Government Should Not Disclose All Vulnerabilities in Its Possession«, *Lawfare*, 7.8.2017, <https://lawfareblog.com/no-us-government-should-not-disclose-all-vulnerabilities-its-possession> (Zugriff am 5.2.2019).

10 Jack Goldsmith, »Cyber Paradox: Every Offensive Weapon Is a (Potential) Chink in Our Defense — and Vice Versa«, *Lawfare*, 12.4.2014, <https://www.lawfareblog.com/cyber-paradox-every-offensive-weapon-potential-chink-our-defense-and-vice-versa> (Zugriff am 5.2.2019).

verwundbar zu halten, bedeutet, dass wir verwundbar bleiben.«[11]

Wenn Staat A also eine Sicherheitslücke zu Spionagezwecken offenhält und diese nicht dem Hersteller meldet, besteht das Risiko, dass ein Akteur B die gleiche Lücke identifiziert und Staat A darüber angreift. Diese Angriffsflächen werden immer größer, da immer mehr billige Computer mit vielen Sicherheitslücken immer mehr Aspekte vernetzter Gesellschaften steuern. »Internet of Things«-Geräte (IoT) steuern automatisierte Fabriken, Stromnetze, Fahrzeuge und in Form von Herzschrittmachern sogar Menschen. Unsichere Software mit 0-Day-Sicherheitslücken ist daher ein globales strukturelles und vor allem kollektives Problem der Cyber-Sicherheit.

11 »There is no way to simultaneously defend US networks while leaving foreign networks open to attack. Everyone uses the same software, so fixing us means fixing them, and leaving them vulnerable means leaving us vulnerable«, Bruce Schneier, »Disclosing vs. Hoarding Vulnerabilities«, *Schneier on Security (Blog)*, 22.5.2014, <https://www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html> (Zugriff am 5.2.2019).

Der Schwachstellen-Lebenszyklus

Wenn das Problem der Schwachstellen von politischer Seite angegangen und unter Kontrolle gebracht werden soll, ist es erforderlich, die Spezifika von Sicherheitslücken näher zu beleuchten. Sicherheitslücken haben verschiedene Existenzzustände, die sich auf einem Spektrum abbilden lassen. Entweder sie sind gänzlich *unbekannt* oder sie sind einem oder mehreren Akteuren *bekannt* (»privat bekannt« bzw. »geheim«) oder sie sind *öffentlich* bekannt. Erfahrungsgemäß haben Sicherheitslücken ein Haltbarkeitsdatum und unterliegen einem Lebenszyklus (siehe Grafik 1, S. 11).

Wie lange dabei die einzelnen Lebensphasen dauern, kann nur grob geschätzt werden, da systematische Studien fehlen. Die Kenntnis der verschiedenen Lebensphasen ist allerdings äußerst wichtig, da sich je nach Phase verschiedene Möglichkeiten der politischen Steuerung ergeben.

Schwachstellen in einer Software müssen zunächst entdeckt werden (»discovery«). Dies geschieht in der Regel durch »code audits«, Penetrationstests (»penetration testing«), Fehlerprüfung (»bug testing«) und sogenanntes Reverse-Engineering von Softwarecode. Informatiker versuchen dabei die Wirkungsweise und das Verhalten von IT-Systemen auf der Code-Ebene nachzuvollziehen. Spezialisierte Teams benötigen je nach Erfahrung und Fähigkeit rund drei Monate intensiver Arbeit, um 0-Days zu entdecken.[12] Der US-Softwareentwickler Symantec schätzt, dass im Jahr 2015 im Schnitt jede Woche eine neue 0-Day-Schwachstelle identifiziert wurde.[13]

Sobald sie eine Sicherheitslücke entdeckt haben, brauchen böswillige Akteure circa einen Monat, um einen funktionierenden Exploit zu entwickeln.[14] Ist der Exploit fertig programmiert und getestet, kann er unmittelbar in der »Wildnis« eingesetzt werden, wie es im IT-Jargon heißt. Ab diesem Moment existiert ein Zeitfenster der Verwundbarkeit (»window of exposure«), in dem der Exploit für Cyber-Operationen genutzt werden kann, ohne dass er von Cyber-Verteidigern entdeckt wird. Im Schnitt dauert es in der Industrie bis zu 200 Tage, bis überhaupt schwerwiegende Cyber-Vorfälle bemerkt werden. Erst dann werden professionelle Incident Response Teams beauftragt, den Angriffsweg zu rekonstruieren und die verwendeten Strategien und Exploits zu analysieren (»Attribution«).

Das so erlangte Wissen um den Vorfall wird dann an den Hersteller der Software gemeldet. Der Prozess der »*Vulnerability Disclosure*« ist von der Internationalen Organisation für Normung (ISO) standardisiert. Dieser Richtlinie zufolge arbeiten Hersteller und Schwachstellenentdecker kooperativ an einer Lösung, um die Sicherheitslücke zu schließen oder die damit verbundenen Risiken zu begrenzen.[15] Das beinhaltet neben der Meldung ein koordiniertes Vorgehen und die Veröffentlichung von Informationen über die Schwachstellen sowie ihre Behebung durch einen Patch. In der Industrie hat sich die Norm herausgebildet, dass ein Hersteller, nachdem er über die Sicherheitslücke benachrichtigt worden ist, rund 90 Tage Zeit hat, den Fehler zu beheben, bevor dieser der Allgemeinheit bekanntgegeben wird. Wenn dieser Zeitraum eingeräumt wird, spricht man von »responsible disclosure«. Erst wenn der Hersteller von der Lücke Kenntnis erhält, kann er mit der Entwicklung eines Patches beginnen. Es vergehen in der Regel 30 bis 60 Tage bis

12 Ablon/Bogart, *Zero Days, Thousands of Nights* [wie Fn. 2], S. 84–87.

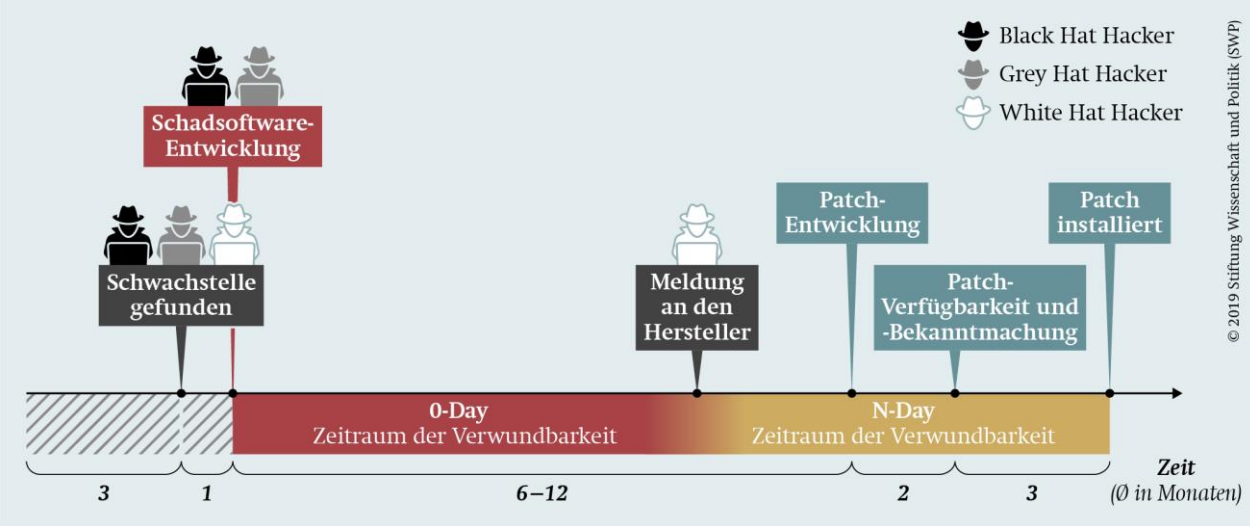
13 »One New Zero-Day Discovered on Average Every Week in 2015«, *Symantec, Press Releases*, 12.4.2016, <www.symantec.com/about/newsroom/press-releases/2016/symantec_0411_01> (Zugriff am 5.2.2019).

14 Ablon/Bogart, *Zero Days, Thousands of Nights* [wie Fn. 2], S. 47.

15 International Organization for Standardization (ISO), *ISO/IEC 29147:2018*, Genf, Oktober 2018, <www.iso.org/standard/72311.html> (Zugriff am 5.2.2019).

Grafik 1

Typischer Lebenszyklus von 0-Day-Schwachstellen



Quelle: Eigene Darstellung, basierend auf Stefan Frei/Bernhard Tellenbach/Bernhard Plattner, *0-Day Patch Exposing Vendors (In)security Performance*, Zürich: ETH [2008], <https://www.blackhat.com/presentations/bh-europe-08/Frei/Whitepaper/bh-eu-08-frei-WP.pdf> (Zugriff am 22.2.2019).

zur Bereitstellung eines Patches (»patch available«).[16] 2017 gab es für rund 86 Prozent aller Schwachstellen einen Tag nach der vollständigen Veröffentlichung der Lücke bereits einen Patch.[17]

Entdeckte Sicherheitslücken werden in der Regel nach dem Common Vulnerabilities and Exposure Standard (CVE) in einer Datenbank veröffentlicht. Sie erhalten eine genormte Identifikationsnummer (zum Beispiel CVE-2010-2729) und Klassifikation, um die Mehrfachregistrierung der gleichen Lücke zu vermeiden und einen reibungslosen Informationsaustausch zwischen IT-Sicherheitspraktikern zu gewährleisten. Diese vollständige Veröffentlichung (»full/public disclosure«) impliziert, dass alle, auch böswillige Hacker, Kenntnis von der Lücke erlangen und entsprechende Exploits schreiben können. Wenn Lücken öffentlich bekannt werden, steigt die Zahl der Schadsoftwarevarianten, die nun diese N-Day-Sicherheitslücke ausnutzen, um ein Vielfaches an. Ziel der übelgesinnten Hacker ist es, das kurze Zeitfenster auszunutzen, bevor alle Nutzer den Patch installiert haben. Daher gilt die vollständige Veröffentlichung einer Sicherheitslücke, bevor der Hersteller einen Patch bereitgestellt hat, als *unverantwortlich*.

Dieser Patch muss dann allerdings noch von den Endnutzern installiert werden. Für ältere Software stellen die Hersteller oft keinen Patch-Support mehr bereit und manche Systeme können aufgrund von Inkompatibilitäten nicht gepatcht werden. Die Industrie braucht im Schnitt noch einmal drei Monate, bis alle Patches installiert worden sind. Darüber hinaus beinhalten rund 10 Prozent der Sicherheitspatches neue Sicherheitslücken, ein Hinweis darauf, dass eine Software niemals 100 Prozent sicher sein kann.[18] Dennoch gibt es Evidenz dafür, dass kontinuierlich weiterentwickelte Software weniger Updates benötigt als zum Beispiel komplette Neuentwicklungen, die in sehr kurzen Zeiträumen erscheinen.[19]

16 »How Long Does It Take to Implement a Patch?«, *Protiviti*, 2017, <www.protiviti.com/US-en/insights/bpro97> (Zugriff am 5.2.2019).

17 Flexera, *Vulnerability Review 2018. Global Trends. Key Figures and Facts on Vulnerabilities from a Global Information Security Perspective*, Itasca, Ill., 2018, <https://bit.ly/2ZclPjE> (Zugriff am 5.2.2019).

18 Leyla Bilge/Tudor Dumitraş, »Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World«, in: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, New York 2012, S. 833–844, <https://doi.org/10.1145/2382196.2382284> (Zugriff am 5.2.2019).

19 Mingyi Zhao/Jens Grossklags/Peng Liu, »An Empirical Study of Web Vulnerability Discovery Ecosystems«, in:

Je kürzer die Lebenszeit einer 0-Day-Sicherheitslücke, desto weniger sinnvoll ist die Verwendung von 0-Day-Exploits für Cyber-Operationen.

In der Regel haben 0-Day-Lücken also eine begrenzte Haltbarkeit und einen »use and loose«-Charakter, was ihren Wert für staatliche Cyber-Operationen mindern kann. Je kürzer die Lebenszeit der Schwachstelle, desto weniger sinnvoll ist eine Verwendung von 0-Day-Exploits für Cyber-Operationen, denn dann besteht die Gefahr, dass bei Einsatz schon ein Patch existiert und der Angriff somit wirkungslos ist. Wie lange 0-Day-Sicherheitslücken »lebendig« bleiben, ist aufgrund einer dünnen Datenlage umstritten. Schätzungen reichen von durchschnittlich 300 Tagen bis hin zu wenigen Jahren.[20] In einer neueren Studie der RAND Corporation wird ein Datensatz mit 200 0-Day-Schwachstellen aus den Jahren 2002—2016 ausgewertet. Die Autoren fanden heraus, dass die durchschnittliche Lebenszeit von 0-Day-Exploits bis zu 6,9 Jahre beträgt. 25 Prozent dieser Exploits werden aber bereits im ersten Jahr in der Wildnis entdeckt und nur weitere 25 Prozent leben länger als 9,5 Jahre.[21]

Wenn Staaten ein Interesse an mehr Cyber-Sicherheit und weniger Sicherheitslücken haben, dann sollten sie Maßnahmen ergreifen, um die einzelnen Zeitfenster zu verkürzen. Je schneller Schwachstellen vom Hersteller behoben werden und je schneller alle Nutzer Patches installieren, desto geringer ist das Zeitfenster der Verwundbarkeit. Dafür gibt es eine ganze Bandbreite von Handlungsoptionen: von rigideren Verpflichtungen für Endnutzer, ihre Systeme zu warten, und für Hard- und Softwarehersteller, zeitnah Updates zu entwickeln, bis hin zu strengeren Regelungen der Herstellerhaftung für IT-Sicherheit. Bevor es darum aber im Detail gehen soll, müssen weitere Faktoren berücksichtigt werden. Dazu gehört zum Beispiel die Frage nach den Akteuren, also danach, wer mit welchen Interessen nach Schwachstellen sucht bzw. daraus Schadsoftware entwickelt.

Das Schwachstellen-Ökosystem: Wer sucht und findet Schwachstellen?

Die Motivation der Akteure zu kennen, die nach Sicherheitslücken forschen und diese ausnutzen, ist elementar für die politische Steuerung des Problems. Neben den Softwareunternehmen, die im Rahmen der schon erwähnten Qualitätskontrolle Sicherheitslücken nachspüren, suchen insbesondere externe IT-Experten, Hacker und (wissenschaftliche) Schwachstellenforscher gezielt nach Fehlern. Diese Akteure lassen sich in jene einteilen, die ein Interesse an der Verbesserung der Sicherheit des digitalen Ökosystems haben und gefundene Schwachstellen melden, und jene, die eigene, oftmals böswillige Absichten verfolgen.

In den letzten Jahren hat sich der Trend durchgesetzt, dass sich Softwarehersteller die Fähigkeiten externer Hacker zunutze machen und diesen im Tausch für das Melden von Schwachstellen eine monetäre Entschädigung und soziale Anerkennung zukommen lassen. Große Firmen wie Facebook, Google und Microsoft nutzen diese sogenannten »Bug-Bounty-Programme« erfolgreich, um die Qualität ihrer eigenen Software zu verbessern.

Da so viele verschiedene Akteure nach Schwachstellen suchen, verschärft sich für staatliche Akteure das oben beschriebene Offensiv-defensiv-Dilemma im Zusammenhang mit 0-Days. 0-Day-Lücken sind nicht einzigartig und können daher separat von mehreren Akteuren gleichzeitig gefunden werden. Das Zurückhalten des Wissens um eine Lücke in der Absicht, diese für staatliche Cyber-Operationen zu nutzen, ist aber nur dann sinnvoll, wenn andere Akteure die gleiche Lücke nicht kennen. Problematisch ist es, wenn zwei oder mehr Organisationen, zum Beispiel Geheimdienste, systematisch die *gleichen* 0-Day-Lücken zurückhalten und ein Exploit-Arsenal anlegen. Da immer mehr Staaten für militärische und nachrichtendienstliche Cyber-Operationen aufrüsten, steigt weltweit die Zahl zurückgehaltener Sicherheitslücken an. Die entscheidende Frage ist, wie groß die Überschneidung dieser Arsenale zwischen Cyber-Akteuren verschiedener Länder ist.

Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, New York 2015, S. 1105—1117, <https://doi.org/10.1145/2810103.2813704> (Zugriff am 5.2.2019).

20 Bilge/Dumitraş, »Before We Knew It« [wie Fn. 18].

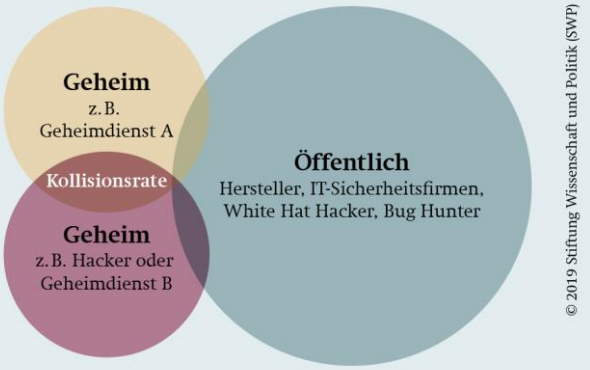
21 Ablon/Bogart, *Zero Days, Thousands of Nights* [wie Fn. 2], S. xi. Das Problem an dieser Studie ist, dass sie auf einem geheimen Datensatz eines nicht genannten Schwachstellenzulieferers der US-Regierung beruht. Der Datensatz ist zudem mit 200 Einträgen zu klein für genaue statistische Berechnungen und vermutlich aufgrund der Singularität der Datenquelle verzerrt, das heißt nicht repräsentativ für andere Akteure.

Akteure des Schwachstellenökosystems

Ein *White-Hat-Hacker* ist ein Spezialist für Computersicherheit, der in geschützte Systeme und Netzwerke eindringt, um deren Sicherheit zu testen und zu bewerten. White-Hat-Hacker nutzen ihre Fähigkeiten, um die Sicherheit zu verbessern, indem sie Schwachstellen aufdecken, bevor böswillige Hacker (bekannt als *Black-Hat-Hacker*) sie erkennen und ausnutzen können.[22] Die Methoden, die sie verwenden, ähneln denen von böswilligen Hackern. Allerdings werden White-Hat Hacker oft von Firmen angeheuert und haben somit die Erlaubnis, Angriffsmethoden zu testen. White-Hat-Hacker werden daher auch ethische Hacker genannt, da ihr Ziel die Verbesserung des IT-Sicherheitsniveaus aller ist. Black-Hat-Hacker haben in der Regel eine böswillige Absicht bzw. verfolgen monetäre oder politische Ziele (zum Beispiel Spionage oder Sabotage). Sie haben kein Interesse daran, Lücken an Hersteller zu melden. Im Bereich zwischen diesen beiden Lagern agieren sogenannte *Grey-Hat-Hacker*, die die von ihnen gefundenen Lücken bzw. Exploits an staatliche Akteure wie Nachrichtendienste oder Strafverfolgungsbehörden verkaufen. Presseberichten zufolge gehören die französische Firma Vupen, die FinFisher GmbH bei München oder das Hacking Team in diese Grauzone der Schadsoftwaredienstleister. Ferner mischen in diesem Markt sogenannte Exploit-Broker mit, die zum Beispiel 0-Days aufkaufen und an Staaten weiterverkaufen. Bekannte Namen in diesem Metier sind die amerikanischen Firmen Vulnerabilities Brokerage International und Netragard oder auch die israelische NSO Group. Sie werden mitunter auch Cyber-Söldner oder digitale Rüstungsunternehmen genannt.[23]

Grafik 2

Kollisionsrate von zurückgehaltenen Sicherheitslücken



Quelle: Darstellung basierend auf Lillian Ablon/Andy Bogart, *Zero Days, Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits*, Santa Monica: Rand Corporation, 2017.

Je größer die Überlappung des Wissens um Sicherheitslücken zwischen den geheim operierenden Akteuren, zum Beispiel zwischen Geheimdiensten (siehe Grafik 2, Gelb und Rot) ist, desto mehr ist die eigene Gesellschaft Risiken gegenüber ausländischen oder anderweitig böswilligen Hackerangriffen ausgesetzt. Der Grad der Überlappung wird Kollisionsrate genannt. Wenn der Geheimdienst A (Gelb) die gleichen Lücken kennt, die ein Geheimdienst B oder ein Black-Hat-Hacker (Rot) für Cyber-Angriffe einsetzt, diese aber dem Hersteller nicht meldet, setzt Gelb die eigene Bevölkerung einem unnötigen Risiko aus, da es ja eigentlich eine effektive Cyber-Verteidigung in Form eines Patches gegen diese Art von Angriffen geben könnte. Je geringer die Überlappung, desto weniger problematisch sind Exploit-Arsenale. Wenn Gelb lediglich seine Kenntnis von Sicherheitslücken zurückhält, die sich auf antiquierte Technologie von Rot beziehen, zum Beispiel auf eine speziell entwickelte Software in Radaranlagen, die bei Gelb nicht existieren, dann ist das Risiko des Zurückhaltens geringer.

Wie groß ist nun tatsächlich die Kollisionsrate? Dadurch, dass Geheimdienste ihre Arsenale in der Regel geheim halten, herrschen hier Intransparenz und Unklarheit. In der bereits zuvor erwähnten RAND-Studie wurde eine durchschnittliche Kollisionsrate von 5,7 Prozent nach einem Jahr festgestellt. Nach 14 Jahren beträgt die Wahrscheinlichkeit, dass zwei Nachrichtendienste die gleiche Schwachstelle gefunden haben, schon rund 40 Prozent.[24] Eine andere Studie geht von einer Kollisionsrate von circa 15 bis 20 Prozent innerhalb des ersten Jahres aus.[25]

22 »White Hat Hacker«, *Techopedia*, <www.techopedia.com/definition/10349/white-hat-hacker> (Zugriff am 5.2.2019), übersetzt durch den Autor.

23 Kim Zetter, »Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales Work«, *Wired*, 24.7.2015, <https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work> (Zugriff am 5.2.2019).

24 Ablon/Bogart, *Zero Days, Thousands of Nights* [wie Fn. 2], S. 43.

25 Trey Herr/Bruce Schneier/Christopher Morris, *Taking Stock: Estimating Vulnerability Rediscovery*, Cambridge, Mass.: Belfer Center for Science and International Affairs, 7.3.2017 (Belfer Cyber Security Project White Paper Series), S. 1,

Das Offensiv-defensiv-Dilemma, das sich im Kontext des Wissens um 0-Day-Sicherheitslücken ergibt, hängt nicht nur von der Lebenszeit der Schwachstellen und der Kollisionsrate ab, sondern auch von der Frage der Grundgesamtheit aller Sicherheitslücken in einem Produkt. Wenn es insgesamt nur *wenige* Sicherheitslücken gibt, steigt die Wahrscheinlichkeit, dass andere Akteure die *gleichen* Lücken finden. In so einem Szenario ist es für Gelb logisch, alle gefundenen Lücken zu beheben und diese somit für Rot ebenfalls nutzlos zu machen, weil auf diese Weise das kollektive Cyber-Sicherheitsniveau steigt. Wenn es aber eine *Vielzahl* verschiedener Lücken gibt, dann steigt die Wahrscheinlichkeit, dass andere Akteure *unterschiedliche* Lücken finden. Damit ist es nicht mehr notwendigerweise der Fall, dass von Gelb gefundene und behobene Sicherheitslücken auch im Arsenal von Rot vorkommen.[26] Responsible Disclosure, also die Benachrichtigung des Herstellers und anschließende Veröffentlichung der Schwachstelle, hätte in einem solchen Szenario einen geringeren Nutzen.

Die Frage, wie viele 0-Days schwarze, graue und weiße Hacker im jeweiligen Besitz haben, kann nicht genau beantwortet werden, da es über die Bestände von Geheimdiensten und Kriminellen kaum Daten gibt. 0-Days machen schätzungsweise zwischen 1 und 10 Prozent aller Schwachstellen aus.[27] Da nicht für jede ein Exploit entwickelt werden kann, legt dies den Schluss nahe, dass die Ressource 0-Days für staatliche Cyber-Operationen bestimmten Limitierungen unterliegt. Wenn mehr weiße als schwarze Hacker nach Schwachstellen suchen, landen weniger Informationen über Lücken auf dem Schwarzmarkt bzw. werden weniger Exploits konstruiert. Je mehr Staaten nach Lücken in den *gleichen* Softwareprodukten suchen, desto größer ist die Wahrscheinlichkeit der Überlappung.

Schwachstellenmärkte: Wer kauft und verkauft Schwachstellen?

Das individuelle Verhalten von Staaten, Firmen und weißen und schwarzen Hackern hat einen Einfluss darauf, wie groß das Problem der 0-Day-Schwachstellen auf der Makroebene ist. Um dieses Verhalten abzubilden, lohnt es sich, den Handel mit 0-Day-Schwachstellen auf Märkten zu betrachten. Ein Handelsplatz ist der legitime *weiße Markt*, zu dem insbesondere die zuvor erwähnten Bug-Bounty- und Vulnerability-Sharing-Programme gehören. Im Rahmen der Letzteren wird das Wissen um 0-Days zu defensiven Zwecken an Organisationen weitergegeben, um etwa Systeme immunisieren zu können (siehe Grafik 3).

Ganz anders verhält es sich auf dem weitgehend unregulierten *Schwarzmarkt*. Hier vertreiben Black-Hat-Hacker Exploit-Kits, Botnetze (»botnet for hire«), Denial-of-Service-Dienste, gestohlene Kreditkarteninformationen, Kundendaten sowie andere illegale Güter und Hacking-Dienstleistungen mit dem Ziel, die erschlichenen Informationen bzw. das gewonnene Know-how für illegale Praktiken zu nutzen. Abnehmer dieser Dienstleistungen sind sowohl Kriminelle, Black-Hat-Hacker, Terroristen als auch Polizeibehörden, Geheimdienste und Militärs nicht nur autoritärer, sondern auch demokratischer Staaten. Der Verkauf von 0-Day-Schwachstellen und Exploits gehört aufgrund der Komplexität dieser »Güter« zu den eher seltenen Premiumdienstleistungen auf dem Schwarzmarkt.[28]

Es wird geschätzt, dass der Schwarzmarkt für Cyber-Kriminalität mit mehreren Milliarden US-Dollar jährlich ein größeres Umsatzvolumen hat als der weltweite Drogenhandel.

Allerdings ist dieser Markt das Haupttriebwerk für verschiedene illegale Cyber-Aktivitäten, die jedes Jahr Milliarden Dollar an wirtschaftlichen Schäden verursachen.[29] Der Markt ist nur schwer zugänglich. Geschäftsbeziehungen basieren häufig auf Vertrauen

<https://doi.org/10.2139/ssrn.2928758> (Zugriff am 5.2.2019). Die Studie hat eine leicht andere Methodologie und analysiert, wie oft Forscher in Sicherheitslückendatenbanken des weißen Marktes die gleichen Lücken melden. Die untersuchten Softwareprodukte waren Chrome, Firefox, Android und SSL.

26 Schneier, »Disclosing vs. Hoarding Vulnerabilities« [wie Fn. 11].

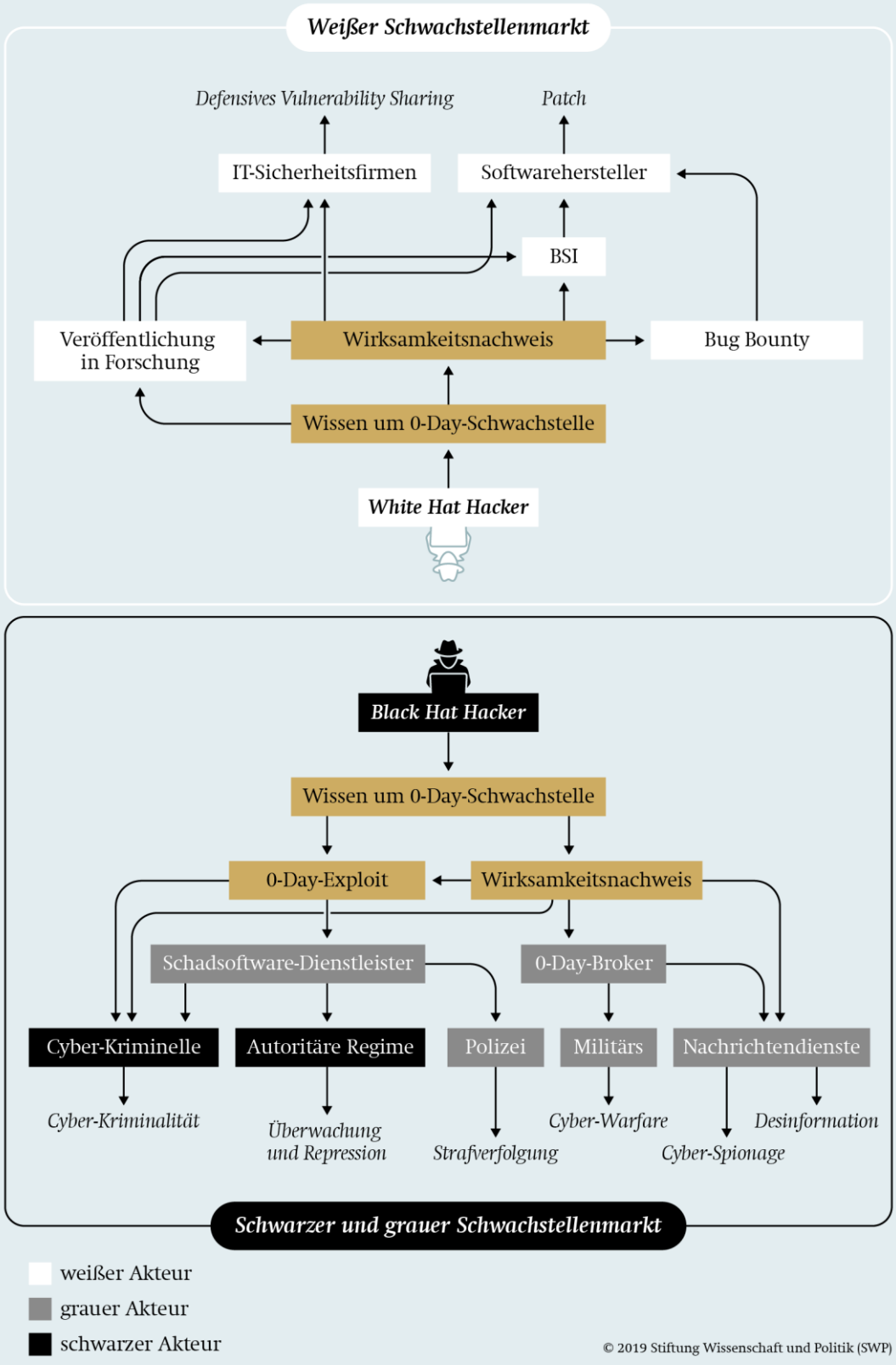
27 Stefan Frei, *The Known Unknowns. Empirical Analysis of Publicly Unknown Security Vulnerabilities*, Austin, Texas: NSS Labs, Inc., 2013 (NSS Labs Briefs), S. 12.

28 Lillian Ablon/Martin C. Libicki/Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data. Hacker's Bazaar*, Santa Monica: Rand Corporation, 2014, S. 1–6, <www.rand.org/pubs/research_reports/RR610.html> (Zugriff am 5.2.2019).

29 Pierluigi Paganini, »The Global Cost of Cybercrime Jumped up to $600 Billion«, *Security Affairs*, 22.2.2018, <https://securityaffairs.co/wordpress/69401/cybercrime/cybercrime-cost-2017.html> (Zugriff am 5.2.2019).

Grafik 3

Verwertungsketten im weißen sowie im schwarzen und grauen Schwachstellenmarkt



und finden über verschlüsselte Direktkontakte (E-Mail, Off-the-record messaging) oder auch in eigenen Foren im Darknet statt.[30] Schätzungen gehen davon aus, dass der Schwarzmarkt für Cyber-Kriminalität mit mehreren Milliarden US-Dollar jährlich ein größeres Umsatzvolumen hat als der weltweite Drogenhandel.[31]

Nicht ganz eindeutig getrennt vom Schwarzmarkt existiert ein *grauer Markt*, auf dem gesetzkonforme IT-Firmen das Wissen um 0-Day-Schwachstellen zum Beispiel an Nachrichtendienste verkaufen oder Schadsoftwaredienstleister dieses Wissen in konfektionierte (»off the shelf«-)Spionageprogramme umwandeln und diese an Strafverfolgungsbehörden veräußern. Dazu gehören Spionagetrojaner, die aus der Ferne Daten von Rechnern auslesen können, aber auch Software zum Knacken verschlüsselter Telefone (zum Beispiel Cellebrite). Die Spionagesoftware FinSpy der in München ansässigen FinFisher GmbH wird laut Presseberichten auch vom deutschen Bundeskriminalamt zur Quellentelekommunikationsüberwachung (»Staatstrojaner«) eingesetzt.[32] Da dieser Markt kaum reguliert ist, machen immer wieder Fälle Schlagzeilen, in denen Firmen entgegen ihrer öffentlichen Bekundungen ihre Dienste an autoritäre Regime verkauft haben. FinSpy wurde zum Beispiel vom Mubarak-Regime in Ägypten 2011 gegen Dissidenten eingesetzt. Ein Insider, der CEO der US-Exploit-Firma Netragard, Adriel Desautels, fordert daher eine Regulierung des grauen Exploit-Marktes: Es gebe dort sehr gierige Leute, »die alles an jeden und zum Teil den gleichen Exploit an mehrere Regierungen verkaufen« und dabei behaupten würden, es handle sich um exklusive Ware. Software wird auf diesen Märkten zur Waffe, die schnell in die falschen Hände gelangen kann und Chaos verursacht, so Desautels.[33]

Daneben gibt es Vermittler, sogenannte Schwachstellen-Broker, die keine Exploits, sondern nur das funktionierende Wissen um 0-Day-Lücken (»Proof of Concept«) verkaufen. Zu den Kunden gehören Schadsoftwaredienstleister, Nachrichtendienste, Advanced-Persistent-Threat-Gruppen und Cyber-Warfare-Einheiten.[34] Aus diesem Grund sind 0-Day-Schwachstellen eine zentrale Ressource in zwischenstaatlichen Cyber-Konflikten. Insbesondere in den USA entwickeln zunehmend auch klassische Rüstungsproduzenten und private Sicherheitsfirmen »Cyber-Waffen«.[35] Wie viele Unternehmen an solchen Tools arbeiten, ist aufgrund hoher Verschwiegenheit nicht bekannt, aber Schätzungen gehen von einer zwei bis dreistelligen Zahl aus.

Wie viele 0-Day-Informationen zirkulieren also auf diesen grauen Märkten? Wegen der Verborgenheit der Geschäftsbeziehungen gibt es naturgemäß kaum öffentliche Zahlen. Als 2015 der italienische Schadsoftwaredienstleister Hacking Team selbst gehackt wurde, erhielt man erstmalig Einblicke in das Innenleben einer solchen Firma.[36] Hacking Team besaß 2015 Kenntnis von sechs 0-Day-Schwachstellen und bot fünf funktionierende 0-Day-Exploits für Strafverfolgungsbehörden an. Hacking Team hatte diese 0-Days zum Teil selber von Freelance-Hackern und größeren Brokern wie der ehemaligen französischen Firma Vupen über nicht-exklusive Verträge gekauft.[37] Käufer können also nicht sicher sein, dass ihre Ware tatsächlich exklusiv ist und nicht eventuell auch von anderen Nachrichtendiensten benutzt wird.

Das US-amerikanische IT-Sicherheitsunternehmen NSS Labs hat in einer Studie Berichte und Verkaufsbroschüren einiger größerer 0-Day-Händler analysiert. Die Firma Endgame bot in der Vergangenheit zum Beispiel ein Portfolio mit 25 0-Day-Exploits für insgesamt 2,5 Millionen US-Dollar an. Der Verkaufspreis

30 Jaziar Radianti/Eliot Rich/Jose Julio Gonzales, »Vulnerability Black Markets: Empirical Evidence and Scenario Simulation«, in: *Proceedings of the 42nd Hawaii International Conference on System Sciences*, Washington, D.C., 2009.

31 Violet Blue, »Hackonomics: ›Cyber Black Market‹ More Profitable than Illegal Drug Trade«, *ZDNet*, 26.3.2014, <https://www.zdnet.com/article/hackonomics-cyber-black-market-more-profitable-than-illegal-drug-trade/> (Zugriff am 5.2.2019).

32 »Smartphone-Überwachung: Grünes Licht für den gekauften Staatstrojaner«, in: *Spiegel Online*, 2.2.2018, <www.spiegel.de/netzwelt/netzpolitik/smartphone-ueberwachung-bka-darf-gekauften-staatstrojaner-jetzt-einsetzen-a-1191112.html> (Zugriff am 5.2.2019).

33 Ryan Gallagher, »Cyberwar's Gray Market. Should the Secretive Hacker Zero-Day Exploit Market Be Regulated?«, *Slate*, 16.1.2013, <https://bit.ly/2IszgXO> (Zugriff am 5.2.2019).

34 Ob diese Unternehmen zum Beispiel auch an den betroffenen Softwarehersteller selbst verkaufen würden, ist wissenschaftlich umstritten.

35 Cyber-Waffen ist ein politisierter Begriff, weshalb hier Anführungszeichen gewählt werden. Die Analogie zu Waffen ist insofern problematisch, als Exploits keine inhärent destruktiven Eigenschaften haben. Exploits sind eher so etwas wie Werkzeuge mit verschiedenen Funktionen.

36 Zetter, »Hacking Team Leak« [wie Fn. 23].

37 Vlad Tsyrklevich, »Hacking Team: A Zero-day Market Case Study«, *tsyrklevich.net*, 22.7.2015, <https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/> (Zugriff am 5.2.2019).

pro Exploit lag zwischen 40 000 und 60 000 US-Dollar. Die Firma Netragard soll 2012 mehr als 50 Exploits an US-Regierungsstellen verkauft haben. NSS Labs schätzt, dass all diese Firmen insgesamt rund 150 Exploits pro Jahr für alle gängigen Softwareprodukte auf den grauen bzw. schwarzen Markt bringen.[38]

Wie funktioniert die Schwachstellenökonomie?

Schwachstellenmärkte sind ökonomischen Zwängen und Wechselwirkungen ausgesetzt, die das Verhalten der Marktteilnehmer beeinflussen und auch einen Ansatzpunkt für politische Steuerung bieten.

Je höher das Cyber-Sicherheitsniveau von Angriffszielen ist, desto kostspieliger werden Cyber-Operationen. Je sicherer Software wird und je mehr lukrative Bug-Bounty-Plattformen auf dem weißen Markt existieren, desto aufwendiger und insbesondere ressourcenintensiver wird das Finden von 0-Day-Schwachstellen für den Schwarzmarkt. Dies hat zur Folge, dass Freelance-Hacker und kleine Teams häufig nicht mehr mit größeren, arbeitsteilig organisierten Firmen konkurrieren können und Personal abgeworben wird, was insgesamt zu einer Konsolidierung des Schwarzmarkts führt.[39] Wie bei rechtskonformen Märkten bestimmen Angebot und Nachfrage auch auf dem schwarzen Markt die Preise für illegale Güter. Die Preise für das Anheuern von Botnetzen sind in den letzten Jahren stark gesunken, weil es mittlerweile so viele Angebote gibt. Preise für gestohlene Kreditkartendaten sinken häufig, wenn ein neues Datenleck den Markt flutet.[40] Ähnliche Dynamiken bestimmen den Handel mit 0-Days. Brokerfirmen wie Zerodium kaufen auf dem grauen Markt einfache 0-Day-Sicherheitslücken, zum Beispiel für das Umgehen von Fingerabdrucksperren auf Smartphones, für bis zu 15 000 US-Dollar. Komplexere Schwachstellen, die das Ausführen von Code aus der Ferne in PDF-Dokumenten erlauben, werden für 500 000 US-Dollar gekauft. Derartige Lücken sind zum Beispiel für die Fernüberwachung von Personen von besonderem Interesse.

38 Stefan Frei/Francisco Artes, *International Vulnerability Purchase Program. Why Buying All Vulnerabilities above Black Market Price Is Economically Sound*, Austin, Texas: NSS Labs, Inc., 2013 (NSS Labs Briefs) S. 10, <https://bit.ly/2VchP3x> (Zugriff am 5.2.2019).

39 Tsyrklevich, »Hacking Team« [wie Fn. 37].

40 Ablon/Libicki/Golay, *Markets for Cybercrime Tools and Stolen Data* [wie Fn. 28], S. 12.

2016 kursierte eine 0-Day-Lücke für iPhones (CVE-2016-4657), die die Übernahme des Geräts aus der Ferne erlaubte, indem einfach eine SMS an das Gerät geschickt wurde. Solche Exploits, die keine Nutzerinteraktionen erfordern und somit gänzlich unbemerkt ein System aus der Ferne infizieren können, sind besonders wertvoll für die Betreiber von Spionage und kosten daher teils Millionenbeträge.[41] Der Großteil der verkauften 0-Days geht für einen Preis zwischen 50 000 US-Dollar und 300 000 US-Dollar über den Ladentisch.

»Die Anreize, Geld für offensive Exploits zu bezahlen, sind größer als die, es in die Verteidigung zu investieren.«

Gemeinhin sind die Preise für 0-Days auf dem Schwarzmarkt weitaus höher als bei vergleichbaren Bug-Bounty- oder Vulnerability-Sharing-Programmen auf dem weißen Markt. Dort belaufen sich die höchstmöglichen Auszahlungssummen, die White-Hat-Hackern für das Melden von Schwachstellen bezahlt werden, auf 20 000 bis — in sehr seltenen Fällen — 200 000 US-Dollar. Die durchschnittlichen Auszahlungssummen der Bug-Bounty-Plattform HackerOne liegen bei circa 2000 US-Dollar. Kritische Sicherheitslücken, die dort nur 9 Prozent der gemeldeten Sicherheitslücken ausmachen, bringen eine Belohnung von im Schnitt 4000 US-Dollar.[42] Aus den geleakten E-Mails des gehackten Schadsoftwaredienstleisters Hacking Team wird ersichtlich, dass die Firma Freelance-Hackern durchschnittlich zwischen 40 000 und 200 000 US-Dollar für Exploits bezahlt hat, die auf dem weißen Markt weniger wert gewesen wären.[43] Auch wenn die konkreten Summen je nach Unternehmen variieren, die Tendenz ist generell wie beschrieben. Casey Ellis, CEO einer Bug-Bounty-Plattform, bezeichnet das Verhältnis des weißen und schwarzen Marktes daher als »ungleiches Spielfeld«: »Die Anreize, Geld für offensive Exploits zu bezahlen, sind größer als die, es in die Verteidigung zu investieren«.[44]

41 »How to Sell Your 0day Exploit to ZERODIUM«, *Zerodium*, <https://zerodium.com/program.html> (Zugriff am 5.2.2019).

42 HackerOne, *The Hacker-Powered Security Report 2018*, San Francisco 2018, <www.hackerone.com/sites/default/files/2018-07/The%20Hacker-Powered%20Security%20Report%202018.pdf> (Zugriff am 5.2.2018).

43 Tsyrklevich, »Hacking Team« [wie Fn. 37].

44 »There's more incentive for people to drop cash on an exploit for offense than for raising defenses«, zitiert in Jose

Diese ungleiche Anreizstruktur schlägt sich in höheren Marktpreisen für 0-Days auf dem Schwarzmarkt nieder: Es wird geschätzt, dass dort die Preise für 0-Days in den letzten zehn Jahren um circa das Fünffache gestiegen sind.[45] Allerdings gibt es dazu keine systematischen Studien. Der Preisanstieg bei 0-Days lässt sich durch eine erhöhte Nachfrage im Zuge des Ausbaus staatlicher Cyber-Warfare-Programme erklären. Gleichzeitig bleibt das Angebot begrenzt, da 0-Days eben verhältnismäßig selten und somit schwer zu finden sind. Wegen der hohen Preise lohnt sich der Einsatz von 0-Day-Exploits oft nur für staatliche bzw. staatsnahe Cyber-Akteure. Für kleinere APT-Gruppen ist es wegen hoher Einkaufskosten häufig sinnvoller, 0-Day-Exploits selbst zu programmieren. Ablon und Bogart schätzen die Kosten der Entwicklung eines 0-Day-Exploits auf rund 30 000 US-Dollar mit einer Bearbeitungszeit von ein bis drei Monaten.[46] Verkäufer auf dem Schwarzmarkt wissen um diese Kaufbereitschaft von Staaten und können daher höhere Preise verlangen.

Wenn Staaten sich Cyber-Sicherheit zum Ziel setzen, müssen sie die Rückkopplungseffekte ihrer offensiven Cyber-Sicherheitspolitik auf das Schwachstellenökosystem beleuchten.

Der US-amerikanische Jurist und Sicherheitsexperte Stephen Maurer kommt zu dem Schluss, dass sowohl die verschobene Anreizstruktur als auch die Kaufbereitschaft der Staaten das primäre Motiv für Hacker ist, statt auf dem weißen lieber auf dem grauen bzw. schwarzen Schwachstellenmarkt aktiv zu sein.[47] Dort ist einfach mehr Geld zu verdienen. Dies wird von Studien bestätigt, die belegen, dass Hacker durchaus bereit wären, Lücken auf dem weißen Markt in Bug-Bounties zu verkaufen, wenn sie dafür Honorare bekämen, die mit denen auf dem Schwarzmarkt konkurrieren könnten.[48] Das Kaufverhalten von Staaten hat also einen Einfluss auf die Marktstruktur. Es bestimmt mit, wie viele Black-Hat-Hacker der Markt »ernährt«, wie viel Schadsoftware von diesen entwickelt wird und somit wie groß das Problem der Cyber-Kriminalität ist. Aus globaler Perspektive betrachtet verschiebt das staatliche Verhalten beim Einkauf von 0-Days das Offensiv-defensiv-Dilemma zugunsten der Offensive oder, wie Ablon und ihre Mitautoren es ausdrücken: »Dank solcher Märkte wird die Fähigkeit zum Angriff wahrscheinlich die Fähigkeit zur Verteidigung übertreffen.«[49]

Wenn Staaten sich also Cyber-Sicherheit zum Ziel setzen, müssen sie die Rückkopplungseffekte ihrer offensiven Cyber-Sicherheitspolitik auf das Schwachstellenökosystem beleuchten. Denn eine offensive Politik vitalisiert den schwarzen Markt und schafft somit Anreize für mehr Cyber-Kriminalität, unter der Staaten leiden. Ein stärkerer Fokus auf die Defensive schafft im Idealfall mehr Anreize für weiße Märkte. Da ungeachtet dieser negativen Rückkopplungseffekte der Trend eindeutig zur Cyber-Offensive geht, ist zu fragen, welche Rolle 0-Days bei staatlichen Cyber-Operationen spielen.[50]

Die Nutzung von 0-Days in staatlichen Cyber-Operationen

Cyber-Operationen, die auf der Ausnutzung von 0-Days basieren, sind bekannte Unbekannte: Wir wissen, dass sie im Geheimen stattfinden, aber wir können sie nicht sehen und daher nur schlecht wissenschaftlich erfassen.[51] Insofern ist es nicht ohne weiteres möglich zu zählen, in wie vielen Cyber-Operationen 0-Days eine Rolle spielen. Berücksichtigt man aber die in den vorherigen Kapiteln erläuterten

Pagliery, »Meet Zerodium, the Company that Pays $1 Million for Apple Hacks«, *CNNMoney*, 7.4.2016, <https://money.cnn.com/2016/04/07/technology/zerodium-apple-hacks/index.html> (Zugriff am 5.2.2019).

45 »The Digital Arms Trade«, in: *The Economist*, 30.3.2013, <https://www.economist.com/business/2013/03/30/the-digital-arms-trade> (Zugriff am 5.2.2019).

46 Ablon/Bogart, *Zero Days, Thousands of Nights* [wie Fn. 2], S. 87.

47 Stephen M. Maurer, »A Market-Based Approach to Cyber Defense: Buying Zero-Day Vulnerabilities«, in: *Bulletin of the Atomic Scientists*, 14.3.2017, <https://thebulletin.org/market-based-approach-cyber-defense-buying-zero-day-vulnerabilities10621> (Zugriff am 5.2.2019).

48 Zhao/Grossklags/Liu, »An Empirical Study of Web Vulnerability Discovery Ecosystems« [wie Fn. 19].

49 «Helped by such markets, the ability to attack will likely outpace the ability to defend«, Ablon/Libicki/Golay, *Markets for Cybercrime Tools and Stolen Data* [wie Fn. 28], S. 31.

50 Matthias Schulze/Sven Herpig, »Germany Develops Offensive Cyber Capabilities without a Coherent Strategy of What to Do with Them«, *Council on Foreign Relations, Blog Post*, 3.12.2018, <https://www.cfr.org/blog/germany-develops-offensive-cyber-capabilities-without-coherent-strategy-what-do-them> (Zugriff am 5.2.2019).

51 Frei, *The Known Unknowns* [wie Fn. 27], S. 10—11.

strukturellen Faktoren (Haltbarkeit, Knappheit, Kollision), dann lässt sich die Verwendung von 0-Days in Relation zu anderen Arten von Cyber-Vorfällen setzen. Nützlich ist hierbei eine Unterscheidung zwischen gezielten Cyber-Attacken, die nur wenige, dafür aber vom Angreifer eigens ausgewählte Hochwertziele betreffen, und automatisierten bzw. opportunistischen Angriffen, die einfach alle verwundbaren Ziele (die sogenannten »low-hanging fruits«) ins Visier nehmen. Gezielte Offensivoperationen sind in der Regel hochspezialisiert und daher komplexer und ressourcenintensiver, während automatisierte Angriffe teils mit einfachen Mitteln, zum Beispiel mit Botnetzen durchführbar sind, die man auf dem Schwarzmarkt mieten kann.

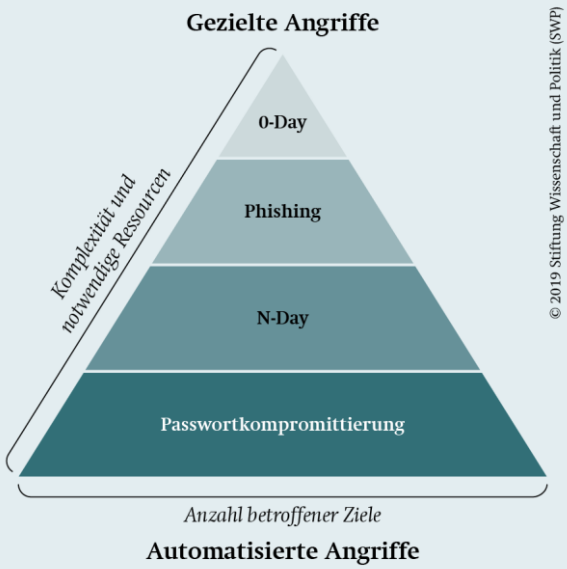
Die weitaus häufigste Erscheinungsform des Cyber-Angriffs sind Fälle von Passwortkompromittierung, also das Übernehmen von Accounts mittels gestohlener oder auf dem Schwarzmarkt gekaufter Nutzerdatenbanken (siehe Grafik 4). Da Nutzer häufig die gleiche Kombination von E-Mail-Adresse und Passwort über mehrere Webseiten hinweg verwenden, kann man mit erschlichenen Logins ganz ohne technisches Hacken Accounts von Websites übernehmen. Diese Form des Identitätsdiebstahls (»credential theft«) kann vollautomatisiert ablaufen und betrifft potentiell Millionen von Opfern. Aber auch in staatlich gesponserten Cyber-Operationen ist das Kompromittieren von Passwörtern eines der gängigsten Instrumente.[52]

Ein Großteil der Cyber-Angriffe im Jahr 2015 nutzte nicht aktuelle, sondern jahrealte, bereits gepatchte Sicherheitslücken aus.

Erst danach kommen klassische Cyber-Angriffe, die *Software-Schwachstellen* ausnutzen, wenngleich es zwischen den Kategorien fließende Grenzen gibt. Innerhalb dieses Bereichs von Cyber-Attacken basieren laut diverser Studien rund 70 Prozent der Vorfälle auf dem Vorhandensein von Sicherheitslücken, für die es bereits Patches gibt, sogenannten N-Days.[53] Der *Verizon Data Breach Report* von 2016 behauptet, dass ein

Grafik 4

Verteilung von Cyber-Angriffen nach Häufigkeit



Quelle: eigene Darstellung basierend auf Alex Stamos, »Black Hat 2017 Keynote«, *Facebook*, 26.7.2017, <www.facebook.com/security/videos/10155111383296886/> (Zugriff am 5.2.2019).

Großteil der Cyber-Angriffe im Jahr 2015 nicht aktuelle, sondern jahrealte, bereits gepatchte Sicherheitslücken ausnutzte.[54] Diese Schwachstellen sind oft »legacy«-Systemen wie Automaten, Anzeigetafeln oder spezialisierten Anwendungen (zum Beispiel medizinische Scanner) eigen, die eine lange Lebensdauer haben und nicht gepatcht werden. Aus diesem Grund ist es hochproblematisch, dass bestimmte IoT-Geräte oder industrielle Kontrollsysteme mitunter über überhaupt keine Update-Mechanismen verfügen und somit bis zum Ende ihrer teils Dutzende Jahre währenden Lebenszeit verwundbar bleiben.

Nach N-Days folgt Phishing. Der zitierte Verizon Report von 2017 zeigt, dass es etwa doppelt so wahrscheinlich ist, dass ein Angriff via »social engineering« gelingt als über das Ausnutzen von 0-Day-Schwachstellen.[55]

52 Bruce Schneier, *Click Here to Kill Everybody. Security and Survival in a Hyper-connected World*, New York 2018, S. 45.

53 »New Research Reveals That 30 Percent of Malware Attacks Are Zero Day Exploits«, *Watchguard*, 30.3.2017, <www.watchguard.com/uk/wgrd-international/news-events/press-releases/new-research-reveals-30-percent-malware-attacks-are> (Zugriff am 5.2.2019).

54 Verizon, *2016 Data Breach Investigations Report*, New York 2016, <www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf> (Zugriff am 5.2.2019).

55 Verizon, *2017 Data Breach Investigations Report*, New York, 26.7.2017, <www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/> (Zugriff am 6.2.2019).

Die zahlenmäßig kleinste Kategorie sind die gezielten *0-Day-Angriffe* auf Hochwertziele, wie zum Beispiel militärische Einrichtungen, Unternehmen mit Schlüsseltechnologien oder sensible Regierungseinrichtungen. Da diese in der Regel gut gesichert sind und Angreifer bei Entdeckung mit politischen Gegenreaktionen rechnen müssen, werden derartige Systeme folglich eher mit schwer detektierbaren 0-Day-Exploits angegriffen.[56] In dieses kleinste Segment von Cyber-Attacken fallen auch APT. Angriffe mit bekannten Sicherheitslücken sind also quantitativ das weitaus größere Phänomen als 0-Day-Angriffe. Letztere sind eher aufgrund ihrer qualitativen Eigenschaften problematisch. Wie ist dies zu erklären?

Hacker wählen in der Regel einen Angriffsweg mit dem besten Kosten-Nutzen-Verhältnis. 0-Day-Attacken sind komplex und erfordern einen hohen Entwicklungsaufwand, da sie für bestimmte Zielkonfigurationen maßgeschneidert werden müssen und dadurch nur schwer wiederverwertbar sind. Für Kleinkriminelle ist es oft lukrativer, bereits bekannte, aber nicht gepatchte Sicherheitslücken auszunutzen, um so mitunter Millionen von Zielen gleichzeitig anzugreifen. Im Gegensatz zu Nachrichtendiensten haben sie weder das Interesse noch das Know-how und die Ressourcen, um längere Zeit in einem System unentdeckt zu bleiben. Staatliche bzw. staatsnahe Akteure verfügen aber über die personellen und finanziellen Mittel für 0-Day-Operationen und haben zudem ein institutionelles Interesse daran, nicht identifiziert zu werden. Dies führt dazu, dass es vorwiegend, aber nicht nur, Geheimdienste und militärische Cyber-Einheiten mit hohem Know-how sind, die 0-Day-Schwachstellen verwenden, um über längere Zeit unentdeckt Hochwertziele auszuspionieren.[57] Prominente Beispiele sind Stuxnet, Duqu und Flame, Operationen, bei denen teils mehrere 0-Day-Sicherheitslücken ausgenutzt wurden. Allgemein lässt sich sagen: Je besser organisiert und finanziert eine Hackergruppe ist, desto größer ist die Wahrscheinlichkeit, dass diese auch 0-Day-Operationen ausführen kann.

Aber auch Staaten unterliegen Kostenzwängen. Der ehemalige Chef der Elite-Hacker-Einheit »Tailored Access Operations« der National Security Agency (NSA), Rob Joyce, erklärte auf einer Konferenz, dass es ein Missverständnis sei, zu glauben, die NSA setze massiv auf 0-Days. Joyce sagte, es sei oft möglich, auch ohne 0-Day-Exploits in große Netzwerke einzudringen, wenn man es nur mit genug Beharrlichkeit versuche.[58] Laut Joyce gehören zu den von der NSA am häufigsten genutzten Angriffsvektoren E-Mails (»spear phishing«), die Kompromittierung bestimmter Websites oder Services (sogenannte Wasserloch-Attacken, »Watering hole attacks«) oder die Infizierung von Datenträgern wie USB-Sticks. Über diese Wege kann mittels N-Days schädlicher Code in ein System geschleust werden. Dies sei in der Summe billiger und weniger risikobehaftet als eine Attacke mit 0-Day-Exploits. Der ehemalige NSA-Mitarbeiter Dave Aitel gibt an, dass es bis zu zwei Jahre dauern kann, bis eine 0-Day-Lücke gefunden und ein vollständig verwendbarer Exploit in eine staatliche Spionageoperation integriert werden kann. Dazu braucht es in der Regel ein Team von 10 bis 40 Personen, die mehrere Monate an einem Angriff arbeiten. Das heißt, der Nutzen von 0-Days unterliegt technischen und operativen Einschränkungen, die dazu führen, dass auch Geheimdienste den oft einfacheren Weg des Angriffs mittels bekannter Sicherheitslücken wählen.[59]

0-Days sind für wirkungsvolle staatliche Cyber-Operationen nicht zwingend erforderlich: N-Days können ähnlich effektiv sein.

Dieser Überblick zeigt, dass Schwachstellen-Governance sich nicht nur auf 0-Days beschränken darf, da sonst große Teile des Problems ignoriert würden. Es wird aber auch deutlich, dass 0-Days nicht zwingend für wirkungsvolle staatliche Cyber-Operationen erforderlich sind, da N-Days ähnlich effektiv sein können.

56 Ablon/Libicki/Golay, *Markets for Cybercrime Tools and Stolen Data* [wie Fn. 28], S. 25.

57 Dave Aitel/Matt Tait, »Everything You Know about the Vulnerability Equities Process Is Wrong«, *Lawfare*, 18.8.2016, <https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong> (Zugriff am 5.2.2019).

58 »I think a lot of people think the nation states, they're running on this engine of zero-days. You go out with your master skeleton key and unlock the door and you're in. It's not that. Take these big, corporate networks, these large networks, any large network — I will tell you that persistence and focus will get you in, will achieve that exploitation without the zero-days«, zitiert in Jessica Conditt, »Zero-Day Exploits Aren't as Important to the NSA as You Think«, *Engadget*, 29.1.2016, <www.engadget.com/2016/01/29/zero-day-exploits-arent-as-important-to-the-nsa-as-you-think/> (Zugriff am 5.2.2019).

59 Aitel/Tait, »Everything You Know about the Vulnerability Equities Process Is Wrong« [wie Fn. 57].

Wie viele Sicherheitslücken werden von Geheimdiensten zurückgehalten?

Da Staaten sowohl die primären Akteure auf dem 0-Day-Markt als auch in Cyber-Konflikten sind, drängt sich die Frage auf, in welchem Umfang sie sich mit dem Wissen um 0-Days bevorratet haben.

Bisher gibt es nur eine Regierung, von der belegt ist, dass sie Informationen über 0-Day-Lücken auf grauen oder schwarzen Märkten eingekauft hat. Aus den geleakten Dokumenten Edward Snowdens ließ sich rekonstruieren, dass die NSA im Jahr 2013 ein Budget von circa 25 Millionen US-Dollar für den Einkauf von Softwareschwachstellen von Privatunternehmen hatte. Dazu kommen die von der NSA bzw. Partnerunternehmen selbst gefundenen Sicherheitslücken. Der ehemalige NSA-Direktor Michael Rogers behauptet, dass die NSA 91 Prozent der Lücken, die sie findet, selbst dem Hersteller meldet.[60] Unklar ist, wie der Geheimdienst mit eingekauften Lücken verfährt. Ausgehend von dem erwähnten Budget und den Marktpreisen von 0-Days kann geschätzt werden, dass die NSA zwischen 100 und 600 0-Day-Schwachstellen pro Jahr einkaufen kann.[61] Der Cybersicherheitsexperte Jason Healey hat auf der Basis dieser Zahlen errechnet, dass die NSA zwischen 15 und 75 0-Days pro Jahr zurückhält.[62] Für die USA hinzuzuaddieren wären noch die von der CIA und dem FBI gehorteten 0-Days. Die *New York Times* benennt zudem Israel, Großbritannien, Russland, Indien und Brasilien als weitere Käufer auf dem grauen Markt.[63]

Wenn man diese Zahlen auf alle Staaten hochrechnet, die gerade Cyber-Warfare Programme aufbauen, ergibt sich theoretisch ein globales Potential einer drei- bis fünfstelligen Zahl von Sicherheitslücken, die den Herstellern gemeldet werden. Zum Vergleich: Eine ebenso fünfstellige Zahl von N- und 0-Day-Lücken wird jährlich der CVE-Datenbank gemeldet (2018: 16 555).[64] Wenn alle 193 Staaten dieser Welt und einige nichtstaatliche Akteure wie Hackergruppen und Schwachstellendienstleister Sicherheitslücken zurückhalten würden, ergäbe sich ein globales Risikopotential von über 100 000 ungemeldeten Verwundbarkeiten. Das wären mehr als alle Lücken, die in den letzten fünf Jahren in der CVE-Datenbank gelistet wurden. Hier zeigt sich, dass die Handlungen der Staaten auf nationaler Ebene negative Effekte auf globaler Ebene erzeugen, die die Cyber-Sicherheit aller gefährden.

60 Sean Lyngaas, »NSA Chief Says Agency Discloses ›91 Percent‹ of Zero Day Bugs«, *FCW*, 9.11.2015, <https://fcw.com/articles/2015/11/09/rogers-zero-days-nsa-lyngaas.aspx> (Zugriff am 5.2.2019).

61 Frei, *The Known Unknowns* [wie Fn. 27], S. 15.

62 Jason Healey, »The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers«, in: *Journal of International Affairs*, 1.11.2016, S. 1–20 (11), <https://jia.sipa.columbia.edu/sites/default/files/attachments/Healey%20VEP.pdf> (Zugriff am 5.2.2019).

63 Nicole Perlroth/David Sanger, »Nations Buying as Hackers Sell Flaws in Computer Code«, in: *New York Times*, 13.7.2013, <www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html> (Zugriff am 5.2.2019).

64 CVE Database, <https://www.cvedetails.com/browse-by-date.php> (Zugriff am 7.2.2019).

Wie sollten Staaten mit Sicherheitslücken umgehen?

Neben dem Einkauf von Lücken auf grauen oder schwarzen Märkten werden in diversen Staaten bereits Research & Development-Einrichtungen aufgebaut, die mittels »reverse engineering« und »penetration testing« selbst eigene Sicherheitslücken finden können und dazu passende Exploits entwickeln sollen. In Deutschland wäre in diesem Zusammenhang die 2016 eingerichtete Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) zu nennen.[65] Geheimdienste verfügen schon seit den frühen 1990er Jahren über eigene Cyber-Abteilungen, die NSA zum Beispiel über die Tailored-Access-Operations-Einheit und die CIA über die Abteilung Cyber-Operations.

Die staatliche Governance von 0-Day-Schwachstellen erstreckt sich insgesamt auf drei Felder: Erstens müssen Staaten eine Haltung zum Bereich der Akquise, also des Einkaufs oder der Eigenentwicklung von Schwachstellen oder Exploits beziehen. Zweitens müssen sie sich zum Problem der Veröffentlichung positionieren, also zu der Frage, ob und wie sie selbst gefundene oder eingekaufte Lücken einem verantwortlichen Meldeprozess unterziehen. Und drittens müssen sie entscheiden, ob und wie Schwachstellen für eigene Cyber-Operationen bzw. staatliches Hacking überhaupt verwendet werden sollen, und antizipieren, welche Effekte dieses Handeln haben könnte.

Staaten, die offensive Cyber-Operationen erwägen, haben im Prinzip drei Optionen für den Umgang mit Sicherheitslücken: Geheimhaltung, vollständige Veröffentlichung oder partielle Veröffentlichung (»Schwachstellenmanagement«).

Geheimhaltung und vollständiges Zurückhalten (stockpiling)

Bisher melden die meisten Staaten, die Cyber-Warfare-Programme aufstellen, Schwachstellen, die sie gefunden haben, nicht, um sie gegebenenfalls in Cyber-Operationen ausnutzen zu können. Das gilt sowohl für demokratische Cyber-Mächte wie Frankreich oder Israel als auch für autoritäre Regime wie China, Iran, Nordkorea oder Russland. Dieses Verhalten lässt sich rational aus den nationalen Sicherheitsinteressen der Staaten ableiten. Gegenwärtig gibt es einen Hype um Cyber-Fähigkeiten. Viele Staaten sehen darin ein Prestigeobjekt und ein Machtmittel zur Erweiterung des eigenen Handlungsspielraums. Die NSA argumentiert, dass das Veröffentlichen von 0-Day-Sicherheitslücken die Möglichkeiten reduziert, wichtige Geheimdienstinformationen im Ausland zu sammeln, terroristische Anschläge zu verhindern, den elektronischen Diebstahl geistigen Eigentums zu unterbinden oder gefährliche Exploits zu finden, die die USA bedrohen.[66]

Aus dieser realpolitischen Perspektive wäre das Melden von Schwachstellen an den Hersteller irrational, da die Entwicklung von Exploits Zeit und Steuergeld verbrennt und nach der Meldung kein »return on investment« mehr zu erwarten wäre. Staaten würden damit zudem indirekt die schlechte Softwarequalität von Herstellern subventionieren.[67] Außer in Berichten von anekdotischer Evidenz bleiben Geheimdienste aber den konkreten Nachweis schuldig, wie wirksam das Verwerten von 0-Days ist.

65 ZITiS-Direktor Wilfried Karl hat über den Kauf und die Entwicklung in der Vergangenheit teils widersprüchliche Aussagen gemacht. Aus einer operativen Logik heraus liegt es aber nahe, dass ZITiS 0-Days entwickeln wird.

66 Lyngaas, »NSA Chief Says Agency Discloses ›91 Percent‹ of Zero Day Bugs« [wie Fn. 60].

67 Aitel/Tait, »Everything You Know about the Vulnerability Equities Process Is Wrong« [wie Fn. 57].

Einseitige Abrüstung und nationale Sicherheit

Befürworter des Zurückhaltens argumentieren, dass das Melden von Lücken durch Geheimdienste an den Softwarehersteller einer unilateralen Abrüstung gleichkäme. Wenn zum Beispiel die USA durch die Offenlegung von Schwachstellen einen Teil ihrer Angriffsfähigkeiten abbauen würden, ohne dass klar wäre, ob Russland, China und andere das Gleiche tun, bedeutete dies einen Verlust an Sicherheit.[68] Die Abrüstung von Dual-use-Wissensressourcen wie 0-Days kann allerdings nur schlecht verifiziert werden. Somit gibt es keine Garantie dafür, dass andere Staaten oder Hackergruppen ebenfalls ihr Verhalten ändern und von ihrer »stockpiling policy« abrücken.

Der stellvertretende NSA-Direktor Rick Ledgett geht sogar noch einen Schritt weiter. Ihm zufolge »würde das Aufgeben dieser Fähigkeiten Menschenleben kosten.«[69] Rob Joyce, der ehemalige Cyber-Security-Koordinator im Weißen Haus, sieht noch einen weiteren Aspekt als wichtig an: 0-Day-Exploits seien ein politisches Mittel der Abschreckung, mit dem man einem Gegner Schaden androhen oder Cyber-Kriminalität aufklären könne. So gesehen schaffe die Existenz von Waffen kein Sicherheitsdilemma, sondern ein Mehr an nationaler Sicherheit. Der Nutzen überwiege hierbei also die Kosten. Die USA könnten es sich nicht erlauben, aus diesem Rüstungswettlauf auszusteigen, da man sonst militärisch ins Hintertreffen gerate.[70]

Spionagevorteil

Die NSA stellt die Vorteile der Nutzung von 0-Days für die eigene Spionagetätigkeit heraus. 0-Days würden es zum Beispiel erlauben, unbemerkt in die Cyber-Kommandos und Nachrichtendienste von Gegnern, aber auch Partnern einzubrechen, um zu beobachten, was diese tun. Diese Art von »aktiver Cyber-Verteidigung« ermöglicht in der Theorie die Generierung von nachrichtendienstlichen Informationen, die dazu befähigen, feindliche Cyber-Angriffe bestimmten Urhebern zuzuordnen. Ferner könne auf der Grundlage solcher Kenntnisse beurteilt werden, welche Angriffstools und Schwachstellen Gegner für welche Ziele benutzen. Dieses Wissen diene wiederum der eigenen Verteidigung. Würde man also auf eigene 0-Day-Operationen verzichten und gefundene Sicherheitslücken an Hersteller melden, verlöre man diese wichtige Quelle der Erfassung von Telemetriedaten.

Cyber-Spionage ist sicherer als andere Spionageformen, da Agenten aus der Ferne globale Datenströme abschöpfen können, ohne sich in Gefahr zu begeben. Cyber-Spionage erlaubt es zudem, weitaus größere und reichhaltigere Datenmengen zu erheben, als die Observation von Zielpersonen im Feld generiert. Moderne Smartphones speichern Bewegungsdaten, biometrische Informationen, Verhaltensdaten und Metadaten und ermöglichen es, wenn sie gehackt werden, so umfangreiche Profile über ihre Besitzer zu erstellen wie kaum ein anderes digitales Gerät. Cyber-Operationen eröffnen der Überwachung somit quantitativ und qualitativ neue Dimensionen.

Der ehemalige NSA-Mitarbeiter Dave Aitel argumentiert daher, dass ein Verbot des Zurückhaltens von 0-Days für Spionageoperationen die Fähigkeit der Geheimdienste, Daten zu sammeln, mindern würde. Dies hätte zur Konsequenz, dass die Dienste verstärkt auf die anlasslose Internetmassenüberwachung setzen würden. Kurzum, die gezielte Tiefenüberwachung mit 0-Days gehe unterm Strich mit einem geringeren Verlust an Privatsphäre einher als die automatisierte, anlasslose Massenüberwachung.[71] Diese Rechnung gilt natürlich nur unter der Voraussetzung, dass gezielte Cyber-Operationen, die 0-Day-Schwachstellen ausnutzen, tatsächlich die Ausnahme bleiben und Massenüberwachung nicht dennoch stattfindet.

Die NSA behauptet, dass die Vorteile, die sich durch die Nutzung von 0-Days für die nationale Sicherheit ergäben, den Verlust an Cyber-Sicherheit ausgleichen würden, der durch das Offenhalten von Lücken entsteht. Die NSA ist sich also bewusst, dass das Geheimhalten von Schwachstellen in der Tat die Cyber-Sicherheit gefährdet. Die Situation, in der man sich befinde, gleiche allerdings der der britischen Codebrecher im Zweiten Weltkrieg, die die Enigma-Chiffriermaschine der Nazis bereits entschlüsselt hatten und daher von gegnerischen Angriffsplänen wuss-

68 Aitel, »Why NSA Critics Are Wrong« [wie Fn. 3].

69 Ledgett, »No, the U.S. Government Should Not Disclose All Vulnerabilities in Its Possession« [wie Fn. 9].

70 Rob Joyce, »Improving and Making the Vulnerability Equities Process Transparent Is the Right Thing to Do«, *The White House*, 15.11.2017, <https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/> (Zugriff am 5.2.2019).

71 Aitel/Tait, »Everything You Know about the Vulnerability Equities Process Is Wrong« [wie Fn. 57].

ten. Um dieses Wissen vor den Nazis zu verbergen, seien absichtlich bestimmte Operationen des Gegners geduldet worden, auch solche, die das Leben alliierter Soldaten in Gefahr brachten. Die Aufrechterhaltung einer solchen Täuschung spielt auch im digitalen Zeitalter eine wichtige Rolle. Die Veröffentlichung von 0-Day-Lücken kann dazu führen, dass der Gegner Informationen über eigene Ziele und Fähigkeiten erlangt. Fremde Geheimdienste könnten aus der Art und Qualität der veröffentlichen Bugs auf spezifische Modalitäten des Reverse-Engineering und somit auf die Programmierfähigkeiten des Dienstes schließen. Ebenso könnte aus solch einer Meldung geschlossen werden, für welche Ziele sich ein Geheimdienst interessiert.[72]

Vollständige, verantwortungsvolle Veröffentlichung

Die zweite Option für den Umgang mit Sicherheitslücken besteht darin, dass Regierungsstellen, die aktiv selbst nach Schwachstellen suchen, diese nach erfolgreicher Entdeckung und Tests an die Hersteller melden. Dies sollte auf verantwortungsvolle Weise geschehen. Das heißt, der Hersteller sollte genügend Zeit bekommen, einen Patch zu entwickeln, bevor die Lücke vollständig veröffentlicht wird. Die Befürworter eines solchen Vorgehens argumentieren, dass sich aus einer Politik des Zurückhaltens von 0-Day-Lücken neue Sicherheitsprobleme ergäben. Daher sei entweder der vollständige Verzicht auf Cyber-Operationen geboten oder alternativ der Verzicht auf Cyber-Operationen, die *lediglich* auf 0-Days basieren. Die sehr häufig auftauchenden N-Day-Schwachstellen könnten dann weiterhin ausgenutzt werden. Glaubwürdig wäre eine Strategie der vollständigen Ächtung von 0-Days aber nur dann, wenn diese auch mit der Selbstverpflichtung einhergehen würde, keine Informationen über Sicherheitslücken auf grauen oder schwarzen Märkten für offensive Zwecke einzukaufen.

Nutzen für Abrüstung und glaubhafte Cyber-Außenpolitik

Staaten, die sich eine Disclosure-Strategie zu eigen machten, würden signalisieren, dass von ihnen als Cyber-Akteur keine Bedrohung ausgeht. Sie würden damit einen Beitrag zur Eindämmung des Rüstungswettlaufs leisten. Aktuelle Forschungsergebnisse zeigen, dass die Akquise von digitalen »Waffen« in Form von 0-Days und Exploits Sicherheitsdilemmata schafft und Rüstungsspiralen auslöst.[73] Insbesondere Cyber-Angriffe auf Regierungseinrichtungen fördern die Unsicherheitswahrnehmung eines Staates. Diese wiederum führt oftmals zu politischem Aktionismus und dem unbedingten Bestreben, notfalls mit gleichen Mitteln zurückschlagen zu können. Eine solche Zielsetzung geht unweigerlich mit der Anschaffung von Cyber-Fähigkeiten und 0-Day-Exploits einher. Diese Art der Aufrüstung wird in Nachbarstaaten wiederum als Bedrohung für die eigene Sicherheit interpretiert, weshalb sie nun auch aufrüsten.

Am Ende eines digitalen Wettrüstens ergäbe sich eine anarchische Situation, in der gut gerüstete Cyber-Mächte und nicht-staatliche Hacker einander auf Augenhöhe bedrohen.

Rüstungswettläufe sind im Cyber-Space nicht auf Staaten in bestimmten geografischen Räumen begrenzt, sondern prinzipiell überregional, da über das Internet jedes Ziel auf dem Globus mit einem Cyber-Angriff attackiert werden kann. Zudem beteiligen sich nicht-staatliche Akteure an diesen Wettläufen. Am Ende eines derartigen digitalen Wettrüstens ergäbe sich weltumspannend eine anarchische Situation, in der gut gerüstete Cyber-Mächte und nicht-staatliche Hacker einander auf Augenhöhe bedrohen.[74] Dies hieße nicht mehr Sicherheit, sondern weniger. Das Denken, das einen solchen Prozess nach sich zieht, kann nur durch unilaterale Beschränkung bzw. Abrüstung und vertrauensbildende Maßnahmen durchbrochen werden.[75]

Eine Cyber-Sicherheitspolitik, bei der die Meldung von Schwachstellen die Regel ist, würde die Soft-Power

72 Schneier, »Disclosing vs. Hoarding Vulnerabilities« [wie Fn. 11].

73 Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*, Oxford 2017.

74 Matthias Schulze/Thomas Reinhold, »Wannacry about the Tragedy of the Commons? Game-Theory and the Failure of Global Vulnerability Disclosure«, in: Audun Jøsang (Hg.), *Proceedings of the 17th European Conference on Cyberwarfare and Security*, Reading 2018.

75 Michael Heller, »Experts Debate Vulnerabilities Equities Process Disclosure«, *SearchSecurity*, 1.8.2017, <https://searchsecurity.techtarget.com/news/450423728/Experts-debate-Vulnerabilities-Equities-Process-disclosure> (Zugriff am 5.2.2019).

von Staaten stärken und hätte den Effekt, dass die kollektive (Cyber-)Sicherheit in Relation zur eigenen digitalen Angriffsfähigkeit als höheres Gut betrachtet wird.[76] Cyber-Sicherheit ist nur global und gemeinsam erreichbar und kann auch nicht gegen andere, sondern nur mit anderen Staaten durchgesetzt werden.

Eine Politik des Meldens von Sicherheitslücken hätte aber noch eine weitere, konkrete Abrüstungsfunktion, die mit einer Eigenheit digitaler Güter zusammenhängt: Anders als bei physischen Waffen würde eine unilaterale Abrüstung in Form des Meldens und Schließens von Sicherheitslücken auch die Abrüstung des Gegners bedeuten, sofern dieser Kenntnis von den gleichen Lücken besitzt.

Kollision, Missbrauch und Diebstahl von Cyber-Arsenalen

Wenn Staaten das Wissen um 0-Day-Sicherheitslücken für eigene Cyber-Operationen zurückhalten, müssen diese Kenntnisse und die Informationen über die jeweiligen Exploits irgendwo gespeichert werden — in Cyber-Arsenalen. Je länger aber 0-Day-Exploits auf Lager liegen, desto größer ist die Wahrscheinlichkeit, dass diese nicht mehr wirkungsvoll sind, wenn sie zum Einsatz kommen — die entsprechenden Sicherheitslücken im Zielsystem könnten in der Zwischenzeit behoben worden sein. Zudem sind 0-Day-Operationen hochgradig auf die Systemkonfiguration eines Ziels maßgeschneidert und können daher nicht einfach gegen komplett anders konfigurierte Ziele gerichtet werden. Stockpiling ist also nur in begrenztem Maße sinnvoll. Offensive Akteure bevorzugen daher die »just in time«-Entwicklung von Exploits.

Dazu kommt das Problem der Kollisionsrate, die größer wird, je mehr Geheimdienste und Strafverfolgungsbehörden am Cyber-Rüstungswettlauf teilnehmen. Staatliche Cyber-Akteure haben überall ein ähnliches Aufgabenspektrum, nämlich die unbemerkte Observation eines Zielsystems über einen möglichst langen Zeitraum. Die Universalität dieses Bestrebens führt dazu, dass sie vorrangig *bestimmte Typen* von 0-Day-Lücken mit bestimmten Qualitätsmerkmalen suchen werden. Der ehemalige Cyber-Security-Koordinator des Weißen Hauses, Howard Schmidt, stellt daher fest, »es sei ziemlich naiv zu glauben, dass man der einzige in der Welt ist, der eine neue 0-Day-Lücke entdeckt hat. Das mag für einige Stunden oder Tage der Fall sein, aber mit großer Sicherheit nicht dauerhaft.«[77]

Ein weiteres Risiko ist, dass Exploits verloren gehen oder gestohlen werden. Ein Arsenal muss hoch gesichert sein, um zu verhindern, dass etwa Innentäter die darin aufbewahrten staatlichen Exploits für eigene Zwecke missbrauchen. Dadurch, dass 0-Day-Angriffe in der Regel nicht detektiert werden können, geht die Speicherung von Exploits mit einem enormen Missbrauchspotential einher. Insider, wie zum Beispiel enttäuschte Mitarbeiter, sind ein oft übersehenes IT-Sicherheitsrisiko.[78] Die diversen Geheimdienstlecks in den USA — von Edward Snowden über Vault 7 bis zu den Shadow Brokern — haben gezeigt, wie real die Gefahr ist. Im Jahr 2017 legte der WannaCry-Ransomware-Vorfall weltweit 250 000 Systeme lahm. Die Informationen über die zugrundeliegende Sicherheitslücke wurden vermutlich aus dem Arsenal der NSA entwendet. Cyber-Arsenale wecken Begehrlichkeiten bei fremden Geheimdiensten. Diese haben ein genuines Interesse daran, die Fähigkeiten ihrer Konkurrenten zu kennen. Da aber IT-Sicherheit ein komplexes Unterfangen ist, können auch die besten Geheimdienste realistischerweise nicht garantieren, dass ihre Systeme vor Hackern sicher sind.

Proliferation und Menschenrechtsverletzungen

Je höher die Nachfrage von Staaten nach 0-Day-Exploits ist, desto mehr davon werden auch auf illegalen Märkten entwickelt und verkauft. Da diese Märkte weitgehend unreguliert sind, können sich auch autoritäre Regime dort bedienen und ihre Cyber-Arsenale aufrüsten. Der ehemalige NSA-Direktor Michael Hayden ist der Ansicht, die amerikanische Teilnahme am Schwarzmarkt führe letztlich dazu, dass US-Steuergelder zugunsten krimineller Geschäftsmodelle ausgegeben würden.[79] Colonel Adams vom US Marine Corps warnte schon vor Jahren, dass der Schwarzmarkt Staaten digital aufrüstet, denen sonst die Fähigkeiten für gezielte Cyber-Operationen fehlen würden.[80] Der WannaCry-Vorfall hat in krasser Weise

76 Schneier, »Disclosing vs. Hoarding Vulnerabilities« [wie Fn. 11].

77 Buchanan, *The Cybersecurity Dilemma* [wie Fn. 73], S. 173, Übersetzung durch den Autor.

78 Verizon, *2017 Data Breach Investigations Report* [wie Fn. 55].

79 »The Digital Arms Trade« [wie Fn. 45].

80 Mailyn Fidler, *Anarchy or Regulation. Controlling the Global Trade in Zero-Day Vulnerabilities*, Stanford, Cal.: Stanford University, Mai 2014, S. 19.

veranschaulicht, wie sehr sich »cyber-power« durch die Proliferation von 0-Days verändern kann.[81] Der Markt betreibt die Proliferation von Exploits und wertet kleinere Akteure, wie Nordkorea, immens auf, ein Land, das aufgrund seiner Isolation sonst kaum das Wissen um komplexe Cyber-Operationen erlangen könnte.[82]

Insbesondere autoritäre Regime setzen 0-Day-Exploits auch zu Menschenrechtsverletzungen ein, indem sie zum Beispiel mit Spionagetrojanern Dissidenten und zivilgesellschaftliche Akteure überwachen. Eindrücklich ist hier das Beispiel des international anerkannten Menschenrechtsaktivisten Ahmed Mansoor, der von den Vereinigten Arabischen Emiraten mit einem 0-Day-Spionagetrojaner überwacht wurde, der aus der Hand des israelischen Dienstleisters NSO Group stammte. Der gleiche Hersteller belieferte über 45 andere, vorwiegend autoritäre Staaten mit ähnlicher Software.[83]

Schwachstellenmanagementprozesse (VEP)

Voraussetzung für ein konstruktives Schwachstellenmanagement ist ein Abstimmungsprozess innerhalb der Exekutive, in dem entschieden wird, ob Geheimdienste, Cyber-Kommandos und Strafverfolgungsbehörden eine *bestimmte Anzahl* von 0-Day-Lücken über einen begrenzten Zeitraum für eigene Zwecke im Interesse der nationalen Sicherheit verwenden dürfen. Der Rest der entdeckten Schwachstellen wäre an den Hersteller zu melden. Eine solche Strategie würde dem Staat, der sie sich zu eigen macht, eine gewisse offensive Fähigkeit für Cyber-Operationen erlauben, im günstigsten Fall aber auch den Anforderungen an die Cyber-Sicherheit gerecht werden. Dafür muss innerhalb einer Regierung ein administrativer Prozess etabliert werden, in dem eine Güterabwägung zwischen offensiven und defensiven Interessen stattfindet. Im Idealfall wird diese Entscheidung von offensiven und defensiven Stakeholdern gemeinsam auf neutralem Boden getroffen, wie in einem Review-Board. Dieses Gremium müsste für jede einzelne 0-Day-Lücke, die von Staaten selbst gefunden, gekauft oder eigens entwickelt wurde, prüfen, ob ein Zurückhalten signifikante Gefahren birgt oder ob die Schwachstelle relativ risikofrei ausgenutzt werden kann. Falls das Risiko zu groß ist, muss die Lücke an den Hersteller gemeldet werden. Solche Verfahren, in denen Staaten die Risiken von Sicherheitslücken abschätzen und deren offensive und defensive Potentiale abwägen, werden gemeinhin als »Government Vulnerability Disclosure Review Process« bezeichnet. In den USA existiert ein solcher »Vulnerability Equities Process« (VEP) seit 2010 und wurde seitdem immer weiter angepasst.[84] Grafik 5 illustriert diesen Prozess.

Für den VEP wurde ein Equities Review Board (ERB) geschaffen, in dem Vertreter all jener Ministerien und nachgeordneten Behörden zusammenkommen, die mit der Sicherheit des Landes betraut sind (unter anderem Ministerien für Innere Sicherheit, Handel, Finanzen, Energie, Verteidigung und die Geheimdienste). Zudem wurden in den Behörden Kontaktgruppen für den regelmäßigen Austausch untereinander eingerichtet, die es jeder Dienststelle erlauben, gefundene 0-Days in den Review-Prozess einzubringen. Anhand einer Liste vordefinierter Kriterien (siehe Box, S. 28) wird abgewogen und dann mit einfacher Mehrheit entschieden, ob die Lücke zum Beispiel für NSA-Cyber-Operationen zurückgehalten oder an den Hersteller gemeldet wird.

Ein Motiv für die Einrichtung des VEP war neben der Schaffung von Transparenz und Legitimität auch die Regulierung der im Verborgenen operierenden Cyber-Warfare-Praktiken nach rechtsstaatlichen Kriterien. Der Prozess sendet zudem an die internationale Gemeinschaft das Signal aus, dass sich die USA im Bereich der digitalen Rüstung selbst Restriktionen auferlegen. Sicherlich ist damit auch die Hoffnung verbunden, eine normative Führungsrolle einzuneh-

81 Gil Baram, »The Theft and Reuse of Advanced Offensive Cyber Weapons Pose a Growing Threat«, *Council on Foreign Relations, Blog Post*, 19.6.2018, <https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat> (Zugriff am 5.2.2019).

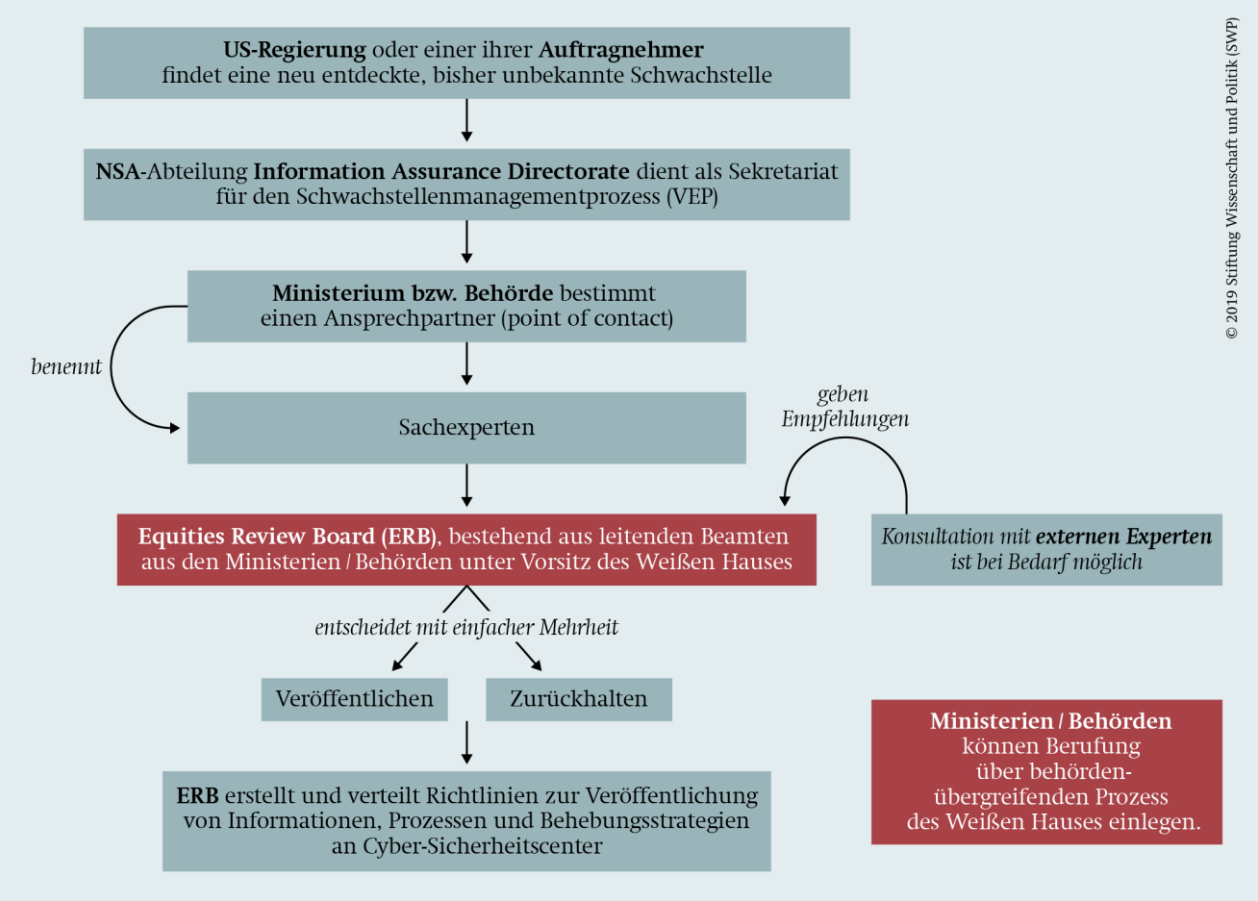
82 Matthias Schulze, »Cyberspace: Asymmetrische Kriegführung und digitale Raubzüge«, in: Hanns Günther Hilpert/Oliver Meier (Hg.), *Facetten des Nordkorea-Konflikts. Akteure, Problemlagen und Europas Interessen*, Berlin: Stiftung Wissenschaft und Politik, September 2018 (SWP-Studie 18/2018), S. 75 – 79.

83 Bill Marczak/John Scott-Railton, »The Million Dollar Dissident. NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender«, *The Citizen Lab*, 24.8.2016, <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/> (Zugriff am 5.2.2019).

84 *Vulnerabilities Equities Policy and Process for the United States Government*, Washington, D.C.: The White House, 15.11.2017, <https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF> (Zugriff am 5.2.2019).

Grafik 5

Der Vulnerability Equities Process« in den USA



Quelle: Eigene Grafik basierend auf Jason Healey, »The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers«, in: *Journal of International Affairs*, 1.11.2016, S. 1—20 (4), <https://jia.sipa.columbia.edu/sites/default/files/attachments/Healey%20VEP.pdf> (Zugriff am 5.2.2019).

men, die andere Staaten zur Nachahmung animieren könnte.[85]

Ein VEP-Prozess ist aber nur sinnvoll, solange er sich an bestimmten Good-Governance-Prinzipien orientiert, zum Beispiel an dem Gebot, die Veröffentlichung von Lücken stets zu priorisieren. Wichtig ist auch, dass im institutionellen Design eines solchen Managementprozesses offensive und defensive Interessen fair ausbalanciert sind, denn die Geheimdienste werden durch ihr Interessenprofil automatisch gegen eine Veröffentlichung von Lücken votieren. Somit gilt es, einen Bias zugunsten einer offensiven Nutzung zu verhindern. Eine solche Verzerrung sollte auch durch die Inklusion zivilgesellschaftlicher Akteure wie Wissenschaftler vermieden werden. Wenn das Wissen über Lücken zurückgehalten wird, sollte diese Entscheidung periodisch neu überprüft werden. Die involvierten Behörden sollten zudem im Dienste der parlamentarischen Kontrolle Transparenzberichte erstellen, aus denen ersichtlich wird, welche Lücken gemeldet und geheim gehalten wurden. Die USA führen seit 2018 darüber hinaus Statistiken über die Zahl der im Review-Prozess behandelten Lücken, denen entnommen werden kann, wie viele Schwachstellen den Herstellern gemeldet und wie viele zurückgehalten wurden.

85 Joyce, »Improving and Making the Vulnerability Equities Process Transparent« [wie Fn. 70].

Die VEP-Kriterien

Die US-Regierung hat 2017 die Kriterien veröffentlicht, die bei der Entscheidung über ein Zurückhalten bzw. eine Meldung einer 0-Day-Lücke eine Rolle spielen. Anbei folgt ein Auszug (Übersetzung durch den Autor):

Teil 1 – Defensive Überlegungen

1.A. Überlegungen zur Bedrohung

- Wo wird das Produkt eingesetzt? Wie verbreitet ist es?
- Wie breit ist die Palette der betroffenen Produkte oder Versionen?
- Ist es wahrscheinlich, dass Bedrohungsakteure diese Verwundbarkeit ausnutzen, wenn sie ihnen bekannt ist?

1.B. Überlegungen zur Verwundbarkeit

- Welchen Zugang muss ein Bedrohungsakteur haben, um diese Schwachstelle auszunutzen?
- Reicht die Ausnutzung dieser Schwachstelle allein aus, um Schaden anzurichten?
- Wie wahrscheinlich ist es, dass Bedrohungsakteure diese Verwundbarkeit entdecken oder davon Kenntnis erhalten?

1.C. Überlegungen zu den Auswirkungen

- Wie sehr verlassen sich die Anwender auf die Sicherheit des Produkts?
- Wie groß ist die Verwundbarkeit? Was sind die möglichen Folgen der Ausnutzung dieser Schwachstelle?
- Welchen Nutzen hat ein Bedrohungsakteur, wenn er diese Schwachstelle ausnutzt?
- Wie hoch ist die Wahrscheinlichkeit, dass Gegner per »reverse engineering« eines Patches die Schwachstelle entdecken und ihn gegen nicht gepatchte Systeme einsetzen?
- Werden genügend Informationssysteme, US-Unternehmen und/oder Verbraucher den Patch tatsächlich installieren, um die potentiellen Sicherheitsschäden abzuwenden?

1.D. Überlegungen zur Risikominderung

- Kann das Produkt so konfiguriert werden, dass diese Schwachstelle minimiert wird? Gibt es andere Mechanismen, um die Risiken dieser Schwachstelle zu minimieren?
- Werden die Auswirkungen einer möglichen Ausnutzung eines 0-Day-Exploits durch bestehende Best-Practice-Richtlinien, Standardkonfigurationen oder Sicherheitspraktiken gemildert?
- Wenn die Schwachstelle gemeldet wird, wie wahrscheinlich ist es, dass der Hersteller oder ein anderes Unternehmen einen Patch oder ein Update entwickelt und veröffentlicht?
- Wenn ein Patch oder Update veröffentlicht wird, wie hoch ist die Wahrscheinlichkeit, dass er auf alle anfälligen Systeme angewendet wird? Wie lange dauert dies? Welcher Prozentsatz der anfälligen Systeme wird auch nach der Veröffentlichung des Patches für immer verwundbar bleiben?
- Können die US-Regierung oder andere Mitglieder der Verteidigungsgemeinschaft erkennen, wenn diese Verwundbarkeit durch Bedrohungsakteure ausgenutzt wird?

Teil 2 – Geheimdienstliche, Strafverfolgungs- und operationelle Abwägungen

2.A. Überlegungen zum operativen Wert

- Kann diese Schwachstelle ausgenutzt werden, um das Sammeln von geheimdienstlichen Informationen und von Beweismitteln für die Strafverfolgung zu unterstützen oder um Cyber-Operationen durchzuführen?
- Welchen Wert hat diese Schwachstelle nachweislich für das Sammeln von geheimdienstlichen Informationen und/oder Beweismitteln für die Strafverfolgung und für die Durchführung von Cyber-Operationen?
- Welches ist der potentielle (zukünftige) Wert dieser Schwachstelle?
- Wie hoch ist die operative Effektivität dieser Schwachstelle?

2.B. Überlegungen zur Wirkungsweise

- Bietet die Ausnutzung dieser Schwachstelle einen spezifischen operationellen Nutzen
  - gegenüber Cyber-Bedrohungsakteuren oder deren Operationen?
  - gegenüber hochrangigen Geheimdienstzielen oder militärischen Zielen?
  - zum Schutz von Soldaten oder Zivilisten?
- Gibt es alternative Mittel, um die operativen Vorteile der Ausnutzung dieser Schwachstelle zu realisieren?
- Würde die Offenlegung dieser Schwachstelle irgendwelche Informationsquellen oder -methoden offenbaren?

Teil 3 – Kommerzielle Überlegungen

- Wenn das Wissen über diese Verwundbarkeit aufgedeckt werden sollte, welche Risiken könnten sich daraus für die Beziehungen der US-Regierung zur Industrie ergeben?

Teil 4 – Internationale Überlegungen

- Wenn das Wissen der US-Regierung über diese Verwundbarkeit aufgedeckt werden sollte, welche Risiken könnten sich daraus für die internationalen Beziehungen ergeben?

Die Metakriterien, die dem VEP zugrunde liegen, orientieren sich vor allem an der Frage, ob eine Lücke wahrscheinlich von einem Gegner ausgenutzt werden kann und wie gefährlich die besagte Lücke ist. Je kritischer eine Lücke und je weiter verbreitet diese ist, desto gefährlicher ist sie. Wenn eine Lücke nicht zuverlässig ausgenutzt werden kann oder eine Software betrifft, die nicht im strategischen Interesse der USA liegt, dann würde das ERB dazu neigen, die Lücke dem Hersteller zu melden. Gleiches gilt, wenn die Lücke in eigenen kritischen Infrastrukturen zu finden ist. Solche Extremfälle sind einfach zu bestimmen. Probleme tauchen dann auf, wenn unklar ist, ob eine Lücke von einem Gegner benutzt wird. Die Amerikaner halten sich hier an das Prinzip »NOBUS — nobody but US«, also an die Devise, niemand außer uns soll Kenntnis von dieser Lücke besitzen. Die zuvor identifizierten

Die VEP-Kriterien (Fortsetzung)

Messschwierigkeiten bei 0-Days machen indes deutlich, dass ein solcher Status einer Schwachstelle kaum zweifelsfrei verifiziert werden kann.

Zudem kann davon ausgegangen werden, dass bei der Entscheidung des ERB noch weitere Fragen eine Rolle spielen. Wie viel Entwicklungskosten und Aufwand haben US-Behörden betrieben um die Lücke zu finden? Je höher die versenkten Kosten, desto mehr wird sich die Waage zur Seite des Zurückhaltens neigen. Was sagt eine veröffentlichte Schwachstelle über das Fähigkeitenlevel der US-Geheimdienste aus? Unklar ist zudem, wie die einzelnen Fragen gewichtet werden.

Analyse und Zusammenfassung

In einer globalisierten Welt benutzen mehr oder weniger alle Staaten ähnliche Hard- und Software (zum Beispiel Windows- oder Mac-PCs mit Intel-Prozessoren oder Smartphones mit Android oder iOS). Auch Regierungen und Militärs benutzen solche Geräte und Systeme. Diese Produkte werden in globalen Lieferketten entwickelt. All das bedeutet, dass sich die Risiken von 0-Days und Hintertüren gleichmäßig auf alle Akteure verteilen. Diese Verflechtung könnte in der Theorie dazu führen, dass Staaten von besonders dramatischen 0-Day-Angriffen absehen, da sie gleichermaßen über solche Angriffe verwundbar sind. Wegen der hochgradigen Verflechtung korreliert das Sicherheitsniveau aller mit dem Melden bzw. Zurückhalten von Sicherheitslücken. Die Annahme, dass eine Meldung von Sicherheitslücken an den Hersteller und das Bereitstellen eines Patches das objektive Cyber-Sicherheitsniveau aller anhebe, basiert auf drei Bedingungen, die sämtlich erfüllt sein müssen.

Trends zur »strategischen Autonomie« könnten eine Asymmetrie der Verwundbarkeitsrisiken noch verschärfen.

Die erste Bedingung ist, dass tatsächlich alle Staaten die gleiche Software verwenden und somit das Risiko gleichmäßig verteilt ist. In der Realität ist das Risiko zum Teil asymmetrisch verteilt: So gibt es in Industrieländern weitaus mehr Einsätze von Computersteuerung an neuralgischen Punkten wie zum Beispiel in Form intelligenter Stromnetze (Smart-Grids), digitaler Wasserversorgung, im Bereich des autonomen Fahrens oder in digitalen Produktionsstätten (Industrie 4.0). Schwellenländer sind somit quantitativ etwas weniger Risiken durch 0-Days ausgesetzt als Industrieländer. Trends zur »strategischen Autonomie« könnten eine Asymmetrie der Verwundbarkeitsrisiken noch verschärfen. Eine Nationalisierung bzw. autonome Eigenentwicklung von Informationstechnik würde dazu führen, dass spezifische Sicherheitslücken ebenso nationalisiert werden. Wenn Staaten komplett unterschiedliche IT-Produkte verwenden, entsteht für Staat A kein Sicherheitsrisiko mehr, wenn er Sicherheitslücken zurückhält, die nur in der nationalen IT von Staat B auftauchen. Die Güterabwägung verschiebt sich in diesem Szenario hin zur Cyber-Offensive.

Die zweite Bedingung ist, dass die Meldung von Sicherheitslücken nur dann zu einem Mehr an Sicherheit führt, wenn die Informationen nicht in falsche Hände geraten, Softwareunternehmen tatsächlich reagieren und schnell Patches bereitstellen und Nutzer diese installieren. Da die durchschnittliche Patch-Zeit nach wie vor drei Monate beträgt, gibt es hier noch viel Verbesserungsbedarf.

Cyber-Sicherheitsexperten und Informatiker plädieren für »responsible disclosure«, während traditionelle Akteure der nationalen Sicherheit für ein Zurückhalten votieren.

Die dritte Bedingung ist, dass durch das Melden der Lücken die Cyber-Arsenale des Gegners auch tatsächlich wirkungslos werden. Diese Bedingung hängt von der Kollisionsrate ab, sprich der Überlappung der Exploit-Arsenale verschiedener Akteure. Bisher gibt es keine solide Evidenz dafür, dass Russen, Chinesen und Amerikaner die gleichen Exploits verwenden. Exploit-Entwicklung ist eine sehr partikulare Angelegenheit. Je diverser Softwareentwicklerteams sind, desto unterschiedlicher sind die Lücken, die sie finden.[86] Systematische Studien zu diesem Aspekt gibt es aufgrund der Geheimhaltung, die den Bereich der digitalen Rüstung naturgemäß umgibt, allerdings nicht.

Sofern also keine Klarheit herrscht, ob diese drei Bedingungen erfüllt würden oder überhaupt erfüllbar sind, lässt sich wissenschaftlich betrachtet die Frage, ob Lücken eher zurückgehalten oder gemeldet werden sollten, nicht eindeutig beantworten. Die Einschätzung, welche Handlungsoption sinnvoller ist,

86 Maurer, »A Market-Based Approach« [wie Fn. 47].

hängt daher maßgeblich vom epistemischen Hintergrund des Bewertenden ab. Cyber-Sicherheitsexperten und Informatiker plädieren einheitlich für »responsible disclosure«, während traditionelle Akteure der nationalen Sicherheit für ein Zurückhalten votieren. Ob die Existenz von offensiven 0-Day-Fähigkeiten aber tatsächlich mit einem Zugewinn an nationaler Sicherheit einhergeht, ist bisher kaum belegt. Wie gezeigt wurde, sind zahlreiche Cyber-Operationen auch ohne den Einsatz von 0-Day-Exploits durchführbar. Insofern scheint die Argumentation der IT-Sicherheitsexperten gegenwärtig stichhaltiger zu sein als die der Geheimdienste, die oftmals keine systematischen Daten liefern, die ihre Position stützen. Deshalb werden im Folgenden Handlungsoptionen aus der Perspektive der IT-Sicherheit entwickelt.

Handlungsoptionen

Das Kernproblem der Cyber-Sicherheit, die mangelnde Qualität von Software und die damit einhergehende Existenz von Sicherheitslücken aller Art, wird in der 2016 verabschiedeten *Cyber-Sicherheitsstrategie für Deutschland* nicht adressiert.[87] Die Wörter »Schwachstelle« oder »0-Day« tauchen darin gar nicht auf. Internationale Partner sind bei der Frage, wie man effektiver mit Sicherheitslücken umgehen könnte, schon weiter. Im Folgenden werden Vorschläge unterbreitet, wie das Problem der Schwachstellen politisch angegangen werden kann, und zwar auf nationaler wie auf internationaler Ebene. Die Vorschläge sind dabei bewusst weit gefasst, insofern als soziale und ökonomische Aspekte miteinbezogen werden. Die hier präsentierten Maßnahmen decken das gesamte Spektrum der oben beschriebenen Schwachstellen-Governance ab: die Konzeptionalisierung der staatlichen Akquise, die Minimierung der Lebenszeit, die Steuerung des Schwachstellen-Ökosystems und die Berücksichtigung und Eingrenzung der internationalen Effekte dieses Systems.

Eine pragmatische Position wäre es, anzuerkennen, dass digitale Rüstungswettläufe weltweit einen Trend zu mehr Cyber-Operationen befeuern. Deutschland hat in den letzten Jahren mit der Schaffung des »Kommandos Cyber- und Informationsraum« und mit der Gründung von ZITiS bereits Fakten geschaffen. Insofern ist es sinnvoll, die bereits vorhandenen offensiven Fähigkeiten einem rechtsstaatlichen Kontrollprozess zu unterwerfen. Die Einführung von Schwachstellenmanagementprozessen auf deutscher, europäischer oder gar internationaler Ebene wäre vor diesem Hintergrund ein sinnvoller Schritt. Im Herbst 2018 hat das Bundesministerium des Innern bekanntgegeben, dass es plant, einen VEP zu initiieren. Auch Großbritannien hat angekündigt, einen VEP zu entwickeln. Eine kürzlich erschienene Studie legt im Detail dar, wie ein effizienter, rechtsstaatlich-transparenter deutscher VEP aussehen könnte.[88] Ein solcher Prozess ist demnach nur sinnvoll, wenn er sich an den zuvor erwähnten Good-Governance-Prinzipien orientiert und »responsible disclosure« als Standardoption definiert. Die Empfehlungen dieser Studie decken sich mit den Erkenntnissen der vorliegenden Untersuchung. Da es bereits weitere wissenschaftliche Analysen gibt, die sich mit der Organisationsstruktur, den Vor- und Nachteilen und den Good-Governance-Leitlinien eines VEP befasst haben,[89] kann hier auf eine detaillierte Darstellung verzichtet werden.

Deutschland hat jedoch jenseits der Einführung eines VEP noch weitere Handlungsoptionen. Die Bundesregierung sollte erwägen, in ihre nächste *Cyber-Sicherheitsstrategie* Instrumente wie Vulnerability-Disclosure-Programme, Bug-Bounties, und Hackerwettbewerbe mit aufzunehmen und Ansätze zu skizzieren, die geeignet sind, den Schwarzmarkt auszutrocknen. Weitere Gegenstände einer solchen Strategie müssten Maßnahmen sein, die sich gegen die oben beschriebenen strukturellen Probleme des Schwachstellenökosystems richten, Maßnahmen also, die

1. den weißen Markt stärken, damit mehr ethische Hacker mobilisiert werden und in mehr Softwareprodukten diversere Arten von Fehlern gefunden werden;
2. die Bedingungen verbessern, dass 0-Day-Schwachstellen schneller entdeckt und behoben werden, damit Software sicherer wird;
3. die Entwicklungskosten für Black-Hat-Hacker in die Höhe treiben, damit sich der Verkauf von

87 Bundesministerium des Innern, *Cyber-Sicherheitsstrategie für Deutschland*, Berlin 2016.

88 Sven Herpig, *Governmental Vulnerability Assessment and Management Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities*, Berlin: Stiftung Neue Verantwortung, August 2018, <https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf> (Zugriff am 5.2.2019).

89 Ari Schwartz/Rob Knake, *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process*, Cambridge, Mass.: Belfer Center for Science and International Affairs, Juni 2016, <www.belfercenter.org/publication/governments-role-vulnerability-disclosure-creating-permanent-and-accountable> (Zugriff am 5.2.2019).

Schwachstellen auf dem Schwarzmarkt weniger lohnt.

Anders als ein Schwachstellenmanagement, das sich auf die Steuerung von Aspekten der staatlichen Akquise von Schwachstellen fokussiert, zielen diese Maßnahmen der Schwachstellen-Governance in erster Linie auf das Schwachstellenökosystem ab. Damit wird nicht nur das Problemfeld 0-Day-Sicherheitslücken adressiert, sondern auch die quantitativ größere Herausforderung der N-Day-Sicherheitslücken. Die Maßnahmen können zunächst auf nationalstaatlicher Ebene umgesetzt werden. Allerdings ist es aufgrund des universellen Charakters der Cyber-Sicherheit geboten, sie auch auf internationaler bzw. auf EU-Ebene anzustoßen. Insofern gelten alle Handlungsempfehlungen immer für Deutschland und die EU.

Verpflichtende Coordinated-Vulnerability-Disclosure-Programme

Der Status quo der Schwachstellen-Governance in Europa wurde 2018 von einer EU-Task Force analysiert. Die Task Force ging von zwei Fragen aus: Sie untersuchte erstens, ob die EU-Mitgliedstaaten »Coordinated Vulnerability Disclosure Policies« (CVD) haben, und zweitens, ob eine »Government Disclosure Policy« existiert. CVD bezeichnet den Prozess des Koordinierens und Teilens von Informationen über Schwachstellen zwischen relevanten Stakeholdern (Entdeckern, betroffenen Firmen, staatlichen Computer Emergency Response Teams [CERTS]) mit dem Ziel, die negativen Effekte von Schwachstellen zu reduzieren und die Öffentlichkeit zu informieren. Eine CVD-Policy impliziert, dass Meldestellen eingerichtet werden, bei denen Forscher gefundene Sicherheitslücken melden können, ohne eine Strafverfolgung fürchten zu müssen. Ferner werden im Rahmen einer solchen Policy die Hersteller in der Regel verpflichtet, die so gemeldeten Lücken nach einer definierten Zeit zu schließen und den Entdecker finanziell oder reputativ zu entlohnen.[90]

Der Begriff »Government Disclosure Policy« bezieht sich auf den Umgang von Regierungsbehörden mit selbst entwickelten oder eingekauften Schwachstellen im Sinne eines VEP.

In Deutschland bzw. besser europaweit sollten CVD-Programme sowohl für den öffentlichen als auch für den privaten Sektor verpflichtend eingeführt werden.[91] Dass es in Deutschland Defizite in diesem Bereich gibt, zeigen die Fälle des elektronischen Anwaltspostfachs[92] oder der Wahlauszählungssoftware des Bundeswahlleiters,[93] deren Betreiber das Wissen um Sicherheitslücken, die ethische Hacker gefunden hatten, in unprofessioneller Weise behandelten. Da mit dem Internet der Dinge auch traditionelle Unternehmen Softwareentwickler oder Internetdienstleister werden, ist die Einführung solcher Programme auch in der Privatwirtschaft geboten. So kann zum Beispiel die Elektronik in normalen Autos genauso über Sicherheitslücken gehackt werden wie industrielle Steuerungsanlagen.

Alle Hersteller oder gewerbliche Betreiber von Software sollten eine Policy entwickeln, die für Externe unmittelbar erkennbar macht, dass sie verantwortungsvoll mit Schwachstellen umgehen, die ihnen gemeldet werden.

CVD-Programme sehen vor, dass jede Organisation, die eigene informationstechnische Systeme (Hard- und Software) besitzt oder herstellt, einen internen Prozess initiiert und etabliert, der die Meldung und Behebung von Schwachstellen in ebendiesen eigenen Systemen zum Ziel hat. Das gilt für die gesamte Cyber-Umgebung, also für selbst entwickelte Software, die angebotenen Dienstleistungen, verwendete Betriebssysteme, IoT-Geräte, Websites oder Hintergrundservices wie etwa Zahlungssysteme. Alle Unternehmen und Organisationen, auf die dies zutrifft, sollten eine Policy entwickeln, die für Externe un-

90 Marietje Schaake/Lorenzo Pupillo/Afonso Ferreia/Gianluca Varisco, *Software Vulnerability Disclosure in Europe. Technology, Policies and Legal Challenges*, Brüssel: Centre for European Policy Studies, Juni 2018, <www.ceps.eu/publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges> (Zugriff am 22.2.2019).

91 Nach *ISO/IEC 29147:2018* und *ISO/IEC 30111*.

92 Volker Weber, »Sicherheitsprobleme beim besonderen elektronischen Anwaltspostfach: Jetzt ist auch das Anwaltsverzeichnis offline«, *Heise Online*, 13.4.2018, <www.heise.de/newsticker/meldung/Sicherheitsprobleme-beim-besonderen-elektronischen-Anwaltspostfach-Jetzt-ist-auch-das-4024204.html> (Zugriff am 5.2.2019)

93 »Software zur Auswertung der Bundestagswahl unsicher und angreifbar«, *Chaos Computer Club*, 7.9.2017, <www.ccc.de/de/updates/2017/pc-wahl> (Zugriff am 5.2.2019).

mittelbar erkennbar macht (zum Beispiel auf der Website), dass der Hersteller oder Betreiber verantwortungsvoll mit Schwachstellen umgeht, die ihm gemeldet werden. Für ethische Hacker sollte schnell ersichtlich sein, wer in der Organisation ein Ansprechpartner zum Melden von Lücken ist (»single point of contact«). Die Organisationen sollten sichere Onlineformulare oder verschlüsselte Kommunikationssysteme zum Melden von Schwachstellen anbieten. Sie müssen sich zudem verpflichten, genügend hausinterne Ressourcen bereitzustellen, um gemeldete Sicherheitslücken zeitnah zu beheben, zum Beispiel einen Chief Information Security Officer samt Entwicklerteam. Eigens dafür geschaffene Einheiten sollten Schwachstellenberichte bearbeiten, die Kommunikation mit dem Melder und öffentlichen Behörden abwickeln und sich dabei mit diesen Akteuren zum Beispiel über Spezifika der Lücke, nächste Schritte und den Zeitpunkt der vollständigen Veröffentlichung verständigen. Institutionen, die solche Teams vorhalten, verringern die Angriffsfläche gegenüber Akteuren, die bekannte, aber noch nicht durch einen Patch behobene N-Day-Sicherheitslücken ausnutzen wollen.

Der Hersteller sollte die in der Industrie üblichen 60 Tage Zeit haben, um einen Patch zu erstellen. Erst danach sollte der Forscher die Lücke veröffentlichen dürfen (für Hardware gelten längere Zeitspannen von sechs Monaten). Der Melder sollte zudem einen zertifizierten Bescheid über die Meldung und über aktuelle Entwicklungsschritte bei der Behebung der Schwachstelle erhalten. Falls die Lücke nicht ohne erheblichen Aufwand geschlossen werden kann, sollte von einer Veröffentlichung abgesehen werden. Die Organisation sollte dem Melder nach Abschluss des Prozesses eine Bug-Bounty-Summe zahlen.

Insbesondere in den Niederlanden und zuletzt auch in der Schweiz wurden mit der verpflichtenden Einführung von CVD-Programmen bereits gute Erfahrungen gesammelt, die als Vorbild dienen können.[94] Das niederländische Modell sieht vor, dass nationale Computer Emergency Response Teams und nationale Cyber-Sicherheitseinrichtungen (wie in Deutschland das Bundesamt für Sicherheit in der Informationstechnik, BSI) in den CVD-Prozess eingebunden werden. Bei staatlichen Organisationen wäre dies generell die vorzuziehende Option, denn das BSI hält die nötigen IT-Ressourcen vor, über die einzelne Behörden in der Regel nicht verfügen. Eine Meldung ist speziell bei bedrohlichen Lücken zu empfehlen, die viele Systeme bzw. kritische Infrastrukturen betreffen. Behörden wie das BSI könnten als Mediatoren oder als Unterstützer der Parteien dienen.

Wirtschaftsakteure sollten Anreize erhalten, CVD-Policies aufzusetzen. Dies könnten finanzielle Anreize, Steuererleichterungen oder Zertifizierungen sein, die den Wert einer Marke erhöhen. Neben diesen Anreizen sollten insbesondere dem BSI aber auch schärfere Sanktionsmaßnahmen an die Hand gegeben werden. Es kommt immer wieder vor, dass Unternehmen nicht reagieren, wenn ihnen Schwachstellen gemeldet werden. In so einem Fall kann das BSI nur mit der Veröffentlichung einer Sicherheitslücke drohen bzw. eine öffentliche Produktwarnung aussprechen. In der Praxis hat sich dieses Sanktionsinstrument aber als nicht praktikabel erwiesen, da die rechtlichen Hürden zu hoch oder nur mühsam zu überwinden sind. Daher sollte dem BSI das Recht übertragen werden, vorgeschaltete Sanktionsmaßnahmen wie Mahnungen oder Bußgelder zu verhängen. Auch damit könnte das Problem der N-Day-Schwachstellen verkleinert werden.

Meldepflichten, etwa bei kritischen IT-Sicherheitsvorfällen, haben sich international bewährt. Daher liegt es nahe, dass der Bundestag im Zuge der Formulierung des nächsten IT-Sicherheitsgesetzes die Verpflichtung zum Melden von Sicherheitslücken an den Hersteller rechtlich verankert. Organisationen ab einem bestimmten Schwellenwert (etwa Firmengröße, Kritikalität der Dienstleistungen, Anzahl der vertriebenen Systeme) sollten per Gesetz dazu motiviert werden, CVD-Prozesse zu initiieren. Dieser gesetzgeberische Akt sollte auch zum Anlass genommen werden, CVD-Policies von Anfang an europaweit zu harmonisieren. Hier wäre das Europäische Parlament gefragt.

Entkriminalisierung ethischen Hackings

Von allen EU-Mitgliedern haben lediglich die Niederlande und Frankreich eine vollständig etablierte CVD-Policy.[95] Dass sich in diesem Bereich noch nicht viel bewegt hat, hängt mit der Budapest-Konvention von 2004 zusammen, die das Hacking partiell kriminalisiert hat. Artikel 2 der Konvention über Cyber-Kriminalität bestimmt, dass die unterzeichnenden Staaten

94 Schaake et al., *Software Vulnerability Disclosure in Europe* [wie Fn. 90], S. 23.

95 Ebd., S. 13.

legislative Maßnahmen ergreifen, um den intentionalen Zugang zu einem System ohne Berechtigung unter Strafe zu stellen. Das bedeutet, dass das unautorisierte Eindringen in Computersysteme oder das Umgehen von Digital-Rights-Management (zum Beispiel BlueRay-Kopierschutz) in vielen EU-Ländern *pauschal* für rechtswidrig erklärt wird. Auch Datenschutz-, Patent- und Copyright-Gesetze enthalten hier und da Klauseln, die Schwachstellenforscher kriminalisieren.[96] Ethische Schwachstellenforscher begehen je nach Auslegung und je nach Land eine strafbare Tat, wenn sie unberechtigt die Sicherheitsmechanismen eines Softwaresystems analysieren und sich mittels einer Schwachstelle Zugang zu diesem System verschaffen können.

Die pauschale Kriminalisierung des Hackings verunsichert die White-Hat-Hacker. Als Folge werden in Europa weitaus weniger Sicherheitslücken an Hersteller gemeldet als in den USA.

Deutschlands Umsetzung der EU-Cybercrime-Konvention stieß auf Kritik. Die Ausweitung des sogenannten Hackerparagraphen 202c des Strafgesetzbuchs (StGB), »Vorbereiten des Ausspähens und Abfangens von Daten«, »schade«, so die Gesellschaft für Informatik in einem Statement im Jahr 2007, »der Informatik, weil jegliche Lehre, Forschung und Entwicklung und selbst die Diskussion über Prüftools zur IT-Sicherheit an Universitäten und Fachhochschulen unter Strafe gestellt werde«.[97] Das Bundesverfassungsgericht urteilte 2009, dass es Ausnahmen für ethische Hackerfirmen im Bereich des »penetrating testing« und für die Forschung und Lehre gebe. Die pauschale Kriminalisierung des Hackings ist einer der primären Beweggründe, warum ethische Hacker keine Schwachstellen melden, weil sie sonst Strafverfolgung befürchten müssten. Sie schürt unter White-Hat-Hackern Unsicherheit, was wiederum dazu führt, dass in Europa weitaus weniger Sicherheitslücken an Hersteller gemeldet werden als zum Beispiel in den USA.[98] Dort setzt sich mittlerweile die Erkenntnis durch, dass CVD-Programme ein essenzieller und effektiver Beitrag für mehr Cyber-Sicherheit sind, weshalb die amerikanische Rechtspraxis zunehmend von einer Strafverfolgung von ethischen Hackern absieht.

Ein Beispiel, wie es gemacht werden kann, ist Lettland. In dem Baltenstaat erwägt man, ethische Hacker von der Haftung freizustellen, wenn sie der CVD-Policy folgen. Haftungsausschlusserklärungen (liability waivers) würden die Hacker vor einer Anklage schützen, falls die Organisation, nachdem eine Schwachstelle gemeldet und behoben wurde, sie verklagen will.[99] Ethische Hacker sind gehalten, die entdeckten Sicherheitslücken dem Softwarebetreiber schnellstmöglich und sicher zu melden, um Risiken zu minimieren. Hacker sollten sich zudem verpflichten, lediglich eine basale, die Verhältnismäßigkeit wahrende Wirksamkeitsprüfung (»Proof of Concept«) einer gefundenen Schwachstelle durchzuführen, nicht aber von den davon betroffenen Systemen sensible Daten zu extrahieren oder eine Schadsoftware zu installieren. Falls diese Verpflichtung nicht eingehalten wird, würde das Agieren des Hackers keiner verantwortungsvollen Offenlegung (»responsible disclosure«) mehr entsprechen und ein strafrechtliches Ermittlungsverfahren nach sich ziehen. Wenn mehrere Forscher unabhängig voneinander involviert sind, sollte eine Koordination stattfinden, um eine frühzeitige Veröffentlichung vor der Fertigstellung eines Patches zu verhindern.[100] Erst nach dem Patch sollten Forscher das Recht haben, die von ihnen identifizierte Lücke der IT-Community bekannt zu machen.

Die Entkriminalisierung des ethischen Hackings und die Schaffung von Rechtssicherheit in Deutschland und Europa haben also hohe Priorität. Der Bundestag sollte hier aktiv werden, um ebendiese Rechtssicherheit für ethische Hacker herzustellen bzw. zu verhindern, dass Hacker pauschal kriminalisiert werden. Auf EU-Ebene sollte das Europäische Parlament die EU-Cybercrime-Konvention entsprechend anpassen.

96 Schneier, *Click Here to Kill Everybody* [wie Fn. 52], S. 41.

97 Detlef Borchers, »Gesellschaft für Informatik befürchtet Kriminalisierung von Informatikern«, *Heise Online*, 3.7.2007, <https://www.heise.de/security/meldung/Gesellschaft-fuer-Informatik-befuerchtet-Kriminalisierung-von-Informatikern-146674.html> (Zugriff am 5.2.2019).

98 HackerOne, *The Hacker-Powered Security Report 2017*, San Francisco 2017, S. 17, <www.hackerone.com/sites/default/files/2017-06/The%20Hacker-Powered%20Security%20Report.pdf> (Zugriff am 5.2.2019).

99 Schaake et al., *Software Vulnerability Disclosure in Europe* [wie Fn. 90], S. 31.

100 Ebd., S. 24–26.

Anreizstrukturen für ethische Hacker: Bug-Bounties und Hackerwettbewerbe

Als weiteres Element auf dem Weg zur Etablierung einer CVD-Policy sollten Maßnahmen ergriffen werden, die stärkere Anreize für ethische Hacker schaffen, gefundene Lücken nicht auf Schwarzmärkten zu verkaufen, sondern diese den Herstellern zu melden.

Die international am meisten verbreitete Variante sind sogenannte »Vulnerability Reward Programs«, Bug-Bounties, die entweder von Softwarefirmen selbst, von Interessenverbänden (zum Beispiel Bugcrowd, HackerOne, Synack) oder von Regierungsstellen initiiert werden. Hacker, die daran teilnehmen, erhalten für jede gemeldete Lücke eine finanzielle Entschädigung und soziale Anerkennung. Die Interessenverbände, die Bug-Bounties organisieren, sammeln Gelder von Mitgliedsfirmen ein, die dann als Preisgeld für jede gemeldete Schwachstelle an Forscher ausgezahlt werden.[101] Die Prämie ist höher, wenn eine Lücke besonders kritisch ist.

Mit Crowdsourcing lässt sich der Mangel an IT-Mitarbeitern zu einem gewissen Teil kompensieren, indem internationale Fachkräfte für die eigene Cyber-Sicherheit mobilisiert werden.

Bug-Bounties sind sinnvoll, denn mit jeder Entdeckung und Meldung nimmt der Bestand an 0-Day-Sicherheitslücken ab. Hacker, die bei externen Bug-Bounties mitmachen, finden mittlerweile ähnlich viele Sicherheitslücken wie In-House-Security-Teams, die Wettbewerbe verursachen aber nur einen Bruchteil der Kosten.[102] Bug-Bounty-Teilnehmer finden zudem andere, diversere Arten von Sicherheitslücken. Der Crowdsourcing-Ansatz ist auf diesem Gebiet auch deshalb geboten, weil im Jahr 2020 weltweit über 1,5 Millionen IT-Sicherheitsexperten fehlen werden. Mit Crowdsourcing können Firmen und Behörden den Mangel an IT-Mitarbeitern zumindest zu einem gewissen Teil kompensieren, indem internationale Fachkräfte für die eigene Cyber-Sicherheit mobilisiert werden.[103] Der Rückgriff auf diese Strategie erfordert allerdings, dass entsprechende Reward-Programme in englischer Sprache vorliegen, dass Bug-Bounties eine firmeninterne Qualitätskontrolle nicht ersetzen und die Programme nicht als bloße Imagekampagne angegangen werden.

Eine andere Möglichkeit, Sicherheitslücken zu finden und zu beseitigen, besteht in der Organisation sogenannter Hackerwettbewerbe. Auf diesen Veranstaltungen müssen Hacker vor einer Jury beweisen, dass sie live die Kontrolle über eine Software oder Hardware übernehmen können. Der so gefundene »Proof of Concept« wird an die betroffene Firma weitergegeben, die die Lücke schließt. Ein Beispiel wäre hier der »Hack the Pentagon«-Wettbewerb, den das US-Verteidigungsministerium 2016 initiierte, nachdem eine Reihe von Datenlecks aufgefallen waren. Über einen Zeitraum von 24 Stunden durften ausgewählte Forscher die Websites des Ministeriums kritisch überprüfen. Sie fanden bei dieser Gelegenheit über 138 Sicherheitslücken, die Pentagon-Spezialisten übersehen hatten.[104]

Das Potential von Hackerwettbewerben lässt sich nur ausschöpfen, wenn es einen Paradigmenwechsel gibt und ethische Hacker als Teil des Immunsystems des Internets verstanden werden.

Damit das Potential solcher Wettbewerbe ausgeschöpft werden kann, muss es einen Paradigmenwechsel geben, in dessen Folge ethische Hacker als Teil des Immunsystems des Internets verstanden werden. Ferner muss sich das Bewusstsein verbreiten, dass ein Verheimlichen von Sicherheitslücken, etwa über »non-disclosure«-Verträge, kontraproduktiv für die Cyber-Sicherheit ist. Ein solcher Wertewandel setzt die Überwindung der Angst voraus, dass mit dem Bekanntwerden von Sicherheitslücken ein Reputa-

101 Jason Reed/Chris Kissel/Tony Massimini, *Analysis of the Global Public Vulnerability Research Market, 2016*, Mountain View, Cal., Juli 2017, S. 11–12, <https://bit.ly/2IP8t79> (Zugriff am 5.2.2019).

102 Matthew Finifter/Devdatta Akhawe/David Wagner, »An Empirical Study of Vulnerability Rewards Programs«, in: Sam King (Hg.), *Proceedings of the 22nd USENIX Security Symposium 2013*, Berkeley, Cal., 2013, S. 273–288, <www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/finifter> (Zugriff am 5.2.2019).

103 BugCrowd, *2018 State of Bug Bounty Report. Bugcrowd's Fourth Annual Report on the Global Crowdsourced Security Economy*, San Francisco 2018, S. 2–5, <https://www.bugcrowd.com/resource/2018-state-of-bug-bounty-report/> (Zugriff am 5.2.2019).

104 Lily Hay Newman, »The Pentagon Opened Up to Hackers — and Fixed Thousands of Bugs«, *Wired*, 10.11.2017, <https://www.wired.com/story/hack-the-pentagon-bug-bounty-results/> (Zugriff am 5.2.2019).

tionsverlust drohe. Dieser droht nur, wenn in Unternehmen keine CVD-Policy und keine Ressourcen existieren, um mit einmal bekannt gewordenen Sicherheitslücken professionell umzugehen. Bug-Bounty-Programme und Hackerwettbewerbe erbringen im Übrigen nicht nur einen funktionalen Sicherheitsgewinn, sie stärken auch das Prestige der veranstaltenden Organisationen, denn sie sind ein Signal für einen aufgeklärten Umgang mit der Schwachstellenproblematik. Weltweit verfügen von den Forbes-Global-2000-Unternehmen nur sechs Prozent über eine CVD-Policy. Die meisten davon sitzen in den USA.[105] Deutschland und Europa hinken hier hinterher.

Der Staat sollte Anreize für höhere Bug-Bounty-Prämien schaffen, damit diese mit den Schwarzmarktpreisen für Schwachstellen konkurrieren können.

Die Bundesregierung sollte also die Förderung von Bug-Bounty-Plattformen und Hackerwettbewerben ganz oben auf ihre Cyber-Sicherheitsagenda setzen. Die EU müsste das Gleiche auf europäischer Ebene tun. Erste diesbezügliche Signale kamen bereits aus Brüssel. Ab Januar 2019 finanziert die EU-Kommission im Rahmen des Projekts »Free and Open Source Software Audit« (FOSSA) Bug-Bounties für 15 Open-Source-Anwendungen.[106] Auch die Bundesregierung kann nationale Bug-Bounty-Programme finanziell unterstützen und bewerben. Bundesbehörden sollten selbstständig Hackerwettbewerbe, zum Beispiel mit Unterstützung des BSI, durchführen. Eine europäisch harmonisierte Lösung wäre von Anfang an zu bevorzugen, damit kein Flickenteppich der Regulierungen entsteht. Die EU-Kommission könnte erwägen, einen Förderfonds für eine europäische Bug-Bounty-Plattform, als Alternative zu amerikanischen Plattformen wie HackerOne, einzurichten. Eine solche Plattform sollte auf einem rechtsstaatlich sicheren Fundament ruhen und technischen, wissenschaftlichen und juristischen Sachverstand integrieren. Die Bildung einer europäischen Bug-Bounty-Plattform wäre auch aus Sicherheitsgründen zu favorisieren, da sich auf diese Weise eher gewährleisten lässt, dass Lücken, die über Bug-Bounty-Plattformen gefunden werden, nicht an die NSA weitergegeben werden — ein Vorwurf der häufig im Raum steht.

Kompetitive Bug-Bounty-Preise

Der Staat sollte zudem Anreize dafür schaffen, dass Bug-Bounty-Prämien höher ausfallen und diese mit den Preisen konkurrieren können, die auf dem Schwarzmarkt für entdeckte Schwachstellen gezahlt werden. Wie gezeigt wurde, gibt es starke finanzielle Anreize für Hacker, das Wissen über die von ihnen gefundenen Sicherheitslücken auf grauen oder schwarzen Märkten zu verkaufen, da der finanzielle Gewinn höher ist als bei einer Meldung an den Hersteller.

Ein Weg, dieses Problem zu lösen, besteht darin, den Auktionsmodus von Bug-Bounties zu verändern. Derzeit legt der Anbieter bzw. der Hersteller bei Bug-Bounty-Programmen fest, welche Summe er zu zahlen bereit ist. Die betriebswirtschaftliche Kalkulation der Firma bestimmt den Preis und nicht die Dynamik des Marktes.[107] Der amerikanische Cyber-Sicherheitsexperte Andy Ozment schlägt daher vor, für Bug-Bounties ein niederländisches Auktionsmodell einzuführen, bei dem ethische Hacker der aufkaufenden Herstellerfirma einen zunächst hohen Preis anbieten und dann sukzessiv niedrigere Angebote machen, bis Forscher und Hersteller sich einig sind.[108]

Das ökonomische Gewicht von Akteuren ist eine Ressource von »cyber-power«, die noch nicht systematisch in die Cyber-Sicherheitspolitik einbezogen wurde. Sie lässt sich aber nutzen.

Die Autoren einer empirischen Untersuchung über Schwachstellenforschung kommen zu dem Schluss, dass Organisationen gut beraten wären, hohe Ausschüttungssummen zumindest in Aussicht zu stellen, da dies nachweislich die Teilnahmebereitschaft erhöht. Dabei macht es keinen Unterschied, ob die durchschnitt-

105 HackerOne, *The Hacker-Powered Security Report 2018* [wie Fn. 42].

106 Kai Schmerer, »EU finanziert Bug-Bounty-Programm für 15 Open-Source-Anwendungen«, *ZDNet.de*, 31.12.2018, <https://www.zdnet.de/88350667/eu-finanziert-bug-bounty-programm-fuer-15-open-source-anwendungen> (Zugriff am 5.2.2019).

107 Rainer Böhme, »A Comparison of Market Approaches to Software Vulnerability Disclosure«, in: Günter Müller (Hg.), *Emerging Trends in Information and Communication Security. ETRICS 2006*, Berlin/Heidelberg: Springer, 2006 (Lecture Notes in Computer Science, Bd. 3995), S. 298–311.

108 Andy Ozment, *Bug Auctions: Vulnerability Markets Reconsidered* (Presented at the Third Workshop on Economics and Information Security), Minneapolis 2004.

lichen Aufkaufpreise unterhalb dieses Höchstwerts liegen.[109] Einige Indikatoren sprechen zudem dafür, dass höhere Belohnungen potentiell die Identifizierung von mehr Sicherheitslücken nach sich ziehen.[110]

Austrocknen des grauen und schwarzen Marktes

Das ökonomische Gewicht von Akteuren ist eine Ressource von »cyber-power«, die bisher nicht systematisch in die Cyber-Sicherheitspolitik einbezogen wurde.[111] Diese Ressource kann genutzt werden, um das Problem des Preisungleichgewichts zwischen weißen und schwarzen Märkten anzugehen. Da das Angebot von 0-Day-Sicherheitslücken auf den Märkten begrenzt ist, kann ein ökonomisch potenter Akteur allein den Markt leerkaufen (Marktmaximierung). Dan Geer, Chief Security Officer bei der CIA-Venture-Capital-Firma In-Q-Tel, ist überzeugt, dass der Aufkauf aller Lücken durch einen Akteur einen Preisanstieg nach sich zöge, der viele Cyber-Kriminelle und weniger wohlhabende Cyber-Akteure vom Schwarzmarkt verdrängen würde. Diese würden dann ein reduzierteres Angebot weniger hochwertiger Schwachstellen zu viel höheren Preisen vorfinden. Für ökonomisch schwache Akteure wäre es dann nicht mehr lukrativ, sich am Schwarzmarkt zu beteiligen.[112]

Die Kosten für das Leerkaufen des Schwarzmarktangebots wären aber für wohlhabende Staaten marginal. Stefan Frei und Francisco Artes haben errechnet, dass beispielsweise die Europäische Union jedes Jahr alle Lücken auf dem Schwarzmarkt für durchschnittlich 150 000 US-Dollar aufkaufen könnte. Ein solcher Betrag würde lediglich 0,01 Prozent des jährlichen Bruttoinlandsprodukts ausmachen.[113] Gleiches gilt für die USA. Das Budget des US-Verteidigungsministeriums für Cyber-Sicherheit beträgt zum Beispiel jährlich 7 Milliarden US-Dollar, womit der Markt bereits mehrfach leergekauft werden könnte.

Zu bevorzugen wäre allerdings, dass Softwarehersteller selbst in die öffentliche Sicherheitsvorsorge einbezogen werden, indem sie die Lücken, die sie selbst betreffen, kaufen und beheben. Wenn nur die größten Softwarehersteller (Apple, Microsoft, Google, Facebook, IBM, Adobe, Cisco, Oracle) alle Lücken auf dem Markt für je 150 000 US-Dollar aufkaufen würden, würde dies ihren individuellen Gewinn nur um 0,044 Prozent schmälern, ein verschwindend geringer Prozentsatz.[114] Verglichen mit den Kosten, die weltweit durch das Ausnutzen von Sicherheitslücken durch Cyber-Kriminelle entstehen, wäre der Aufkauf durch Unternehmen die sinnvollere Option. Dies hat auch damit zu tun, dass in der digitalen Ökonomie Netzwerkeffekte sichtbar sind: Eine geringe Zahl von Firmen ist aufgrund ihrer marktdominanten Stellung in einzelnen Bereichen (Betriebssysteme, Suche, Office-Anwendungen, Server etc.) für den Großteil aller Sicherheitslücken verantwortlich. Gleichzeitig sind dies die Firmen mit den größten jährlichen Gewinnen, teils jenseits der Milliardenmarke. Die Umwälzung der Kosten für Schwachstellen auf die Hersteller ist schon allein deshalb ratsam, weil diese in allen Phasen des Schwachstellenlebenszyklus in einer dominanten Handlungsposition sind.

In der Forschung ist umstritten, ob eine Politik der Marktmaximierung (Leerkaufen des Marktes durch Staaten) oder Marktminimierung (keine staatliche Marktteilnahme) ökonomisch sinnvoller ist. Da ein derartiger Eingriff in Märkte unbeabsichtigte Effekte haben kann, wäre es empfehlenswert, zunächst eine internationale Expertenkommission einzurichten, die die möglichen Folgen einer solchen Regulierung in Form einer Marktmaximierung oder Marktminimierung analysiert. Dieser Kommission sollten zivile Ökonomen und IT-Sicherheitsexperten angehören. Die EU-Kommission oder die deutsche Bundesregierung könnten eine solche Kommission ins Leben rufen.

Damit eine Politik der Marktmaximierung die erwünschten Resultate hervorbringt, müssten die gekauften Lücken aber zwingend an den Hersteller gemeldet und von diesem möglichst geschlossen werden. Die erwartbaren Widerstände gegen das hier beschriebene Vorgehen sind allerdings weniger ökonomisch als politisch begründet: Geheimdienste, Militär und Strafverfolgungsbehörden weltweit sind eine bremsende Kraft, wenn es um die Regulierung internationaler Schwachstellenmärkte geht.

109 Finifter/Akhawe/Wagner, »An Empirical Study of Vulnerability Rewards Programs« [wie Fn. 102].

110 Frei/Artes, *International Vulnerability Purchase Program* [wie Fn. 38], S. 14.

111 Joseph S. Nye, *The Future of Power*, New York 2011, S. 113.

112 Maurer, »A Market-Based Approach« [wie Fn. 47].

113 Frei/Artes, *International Vulnerability Purchase Program* [wie Fn. 38], S. 2.

114 Ebd., S. 16.

Fazit

Um das Kernproblem der Cyber-Sicherheit — Sicherheitslücken — in den Griff zu bekommen, müssen Staaten eine eindeutige Position zu der Frage beziehen, wie sie mit digitalen Verwundbarkeiten umgehen wollen. Dabei gilt es, verschiedene Interessen abzuwägen, nämlich das enge Konzept nationaler Sicherheit, das insbesondere von offensiven Cyber-Akteuren vertreten wird, gegen das globale, kollektive Bedürfnis nach Cyber-Sicherheit und dem Beseitigen von Schwachstellen. Ferner muss das Streben nach kurzfristigem Gewinn mit dem nach langfristiger Sicherheit austariert werden. Die Studie hat gezeigt, dass an das Thema ein größerer Maßstab angelegt werden muss. Soziale, ökonomische, außen- und sicherheitspolitische Faktoren spielen eine Rolle. Ferner ist eine Fokussierung lediglich auf 0-Day-Sicherheitslücken zu eng. N-Day-Schwachstellen müssen mitbedacht werden.

Eine wichtige Frage, die aufgrund ihrer Komplexität hier nicht diskutiert wurde, ist auch die der Herstellerhaftung bei Software. Der Umstand, dass Softwareunternehmen, anders als Automobilhersteller, nicht für die Sicherheit ihrer Produkte haften müssen, trägt dazu bei, dass der Softwaremarkt dysfunktional ist, denn er schafft keine Anreize für sichere Softwareentwicklung.[115] Die Erkenntnis, wie interdependent diese einzelnen Faktoren des Schwachstellenökosystems sind, zwingt zu dem Schluss, dass sich dieses Problem nur global lösen lässt. Insofern hat das Thema Cyber-Sicherheit einige Ähnlichkeit mit den globalen Abrüstungsbemühungen im Kalten Krieg, die einen Schub erhielten durch den Paradigmenwechsel weg von der Fokussierung auf eine einseitig nationale und hin auf kollektive Sicherheit. Da die Bearbeitung der Sicherheitslückenproblematik in Deutschland bisher fast ausschließlich im Bereich der inneren Sicherheit angesiedelt ist, ist die internationale Betrachtung dieser Herausforderung in Deutschland vergleichsweise unterentwickelt.

Daher sollten in Zukunft neben den hier formulierten Vorschlägen für nationale bzw. europäische Lösungsansätze (Entkriminalisierung von White-Hat-Hacking, Förderung von Bug-Bounties und Hackerwettbewerben, markante Erhöhung der Bug-Bounty-Preise, Etablierung von Coordinated-Vulnerability-Disclosure-Programmen und Austrocknen des Schwarzmarkts) auch internationale Kooperationsbemühungen ausgelotet werden. Die Diskussionen über ein multilaterales Regime zur Begrenzung von 0-Days (International Vulnerability Equities Program) stecken bisher noch in den Anfängen und werden von dem Umstand gehemmt, dass viele Staaten bisher einen größeren Vorteil darin sehen, ihr Wissen um Sicherheitslücken für offensive Cyber-Operationen zurückzuhalten. Neben dem fehlenden politischen Willen gibt es auch Probleme bei der Attribution (Rückverfolgung) von Cyber-Vorfällen. Die Debatte über die Regulierung von Cyber-Angriffen auf der Ebene der Vereinten Nationen ist daher bisher nicht weit vorangekommen. Existierende Abkommen wie das Wassenaar-Arrangement zur Begrenzung des Exports von Überwachungssoftware sind ein erster Schritt. Sie haben aber bisher nur geringe Verbindlichkeit.[116]

Gleichzeitig wächst innerhalb der Staatengemeinschaft das Bewusstsein dafür, dass Angriffe auf kritische Infrastrukturen besonders bedrohlich sind. Da derartige Attacken in der Regel mit 0-Day-Exploits durchgeführt werden, wäre die Ächtung ebensolcher 0-Day-Exploits für Cyber-Operationen also potentiell ein kleinster gemeinsamer Nenner für ein internationales Regime zur Eindämmung der Schäden von Cyber-Vorfällen. Wenn Staaten nun damit beginnen, in ihrem Souveränitätsbereich Schwachstellenmanagementprozesse zu initiieren, könnte gleich mit darüber nachgedacht werden, wie ein ähnlicher Prozess auf europäischer, Nato- oder gar globaler Ebene aussehen könnte.

115 Böhme, »A Comparison of Market Approaches to Software Vulnerability Disclosure« [wie Fn. 107].

116 Fidler, *Anarchy of Regulation* [wie Fn. 80], S. 135.

Abkürzungen

APT	Advanced Persistent Threat
BSI	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
CVD	Coordinated Vulnerability Disclosure Policies
CVE	Common Vulnerabilities and Exposure Standard
ERB	Equities Review Board
FOSSA	Free and Open Source Software Audit
IoT	Internet of Things
NSA	National Security Agency
VEP	Vulnerabilities Equities Process
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Literaturhinweise

Matthias Schulze
Kriminalitätsbekämpfung im Dark Net. Neue Ermittlungsansätze statt Verbote
SWP-Aktuell 28/2019, April 2019
doi:10.18449/2019A28

Annegret Bendiek/Matthias Schulze
Desinformation und die Wahlen zum Europäischen Parlament
SWP-Aktuell 10/2019, Februar 2019
doi:10.18449/2019A10

Matthias Schulze
»Cyberspace: Asymmetrische Kriegführung und digitale Raubzüge«, in: Hanns Günther Hilpert/Oliver Meier (Hg.), **Facetten des Nordkorea-Konflikts. Akteure, Problemlagen und Europas Interessen**
SWP-Studie 18/2018, September 2018, S. 75—79

Matthias Schulze
Hacking back? Technische und politische Implikationen digitaler Gegenschläge
SWP Aktuell 59/2017, August 2017

Im SWP-Themendossier **»Digitalisierung–Cyber–Internet«** findet sich eine annotierte Bibliographie zum Thema Schwachstellen/Sicherheitslücken
https://www.swp-berlin.org/index.php?id=2320